Sentinel 4.0 User Interface Guide

A quick primer on the available options of the Sentinel's web-based user interface.

Navigation Header

This header will remain at the top of the page even if you need to scroll, and contains the following items:

- **Navigation links:** Contains the top-level links for the interface, as described in detail below.
- **Current user:** Displays your username. Click on your username to access links to your profile and log out of the system.
- **Current time:** Displays in military time (24-hour format), in the current time zone (which defaults to US Central time). Click the time to edit the system time zone.
- **Find an IP tool:** Enter an IPv4 IP in to this box, and press Enter. This will take you directly to that IP's detail page, which gives a summary of activity and a timeline of everything that has ever happened on your network related to that IP, including events, blocks, releases, configuration changes, and dropped packets.

Title Bar

This is the grey bar directly underneath the navigation header. It always contains:

- The system's current **Location** and **Organization**. This is editable by navigating to Configuration -> Organizational Info.
- The right-hand side shows important messages, and displays the **current mode** of the Sentinel. If there are pending **configuration items**, a red banner will display here, reminding you to commit your configuration changes. Also, if there are any **'Flagged' events** – events that are serious enough that you should act upon them immediately – a black banner with a red flag will display here. You can click on each of these items for more detail, as necessary.

Dashboard

This is the system's effective home page. It refreshes once an hour, and displays:

- The number of **current blocked networks** in the upper right corner.
- A chart of activity over time and summarized by severity, and some basic statistics. You may choose to display the last 24 hours, last 7 days, last 30 days, or all activity. You can also click on the legend to hide or show different severities.
- Below the chart and network statistics, the dashboard displays various **configuration settings** and other 'housekeeping' items, like configuration time, signature update, and software version.

Blocked Networks

Probably the most visited and most important function on the interface. This is where you go to manage your false positives; hopefully, these are few and far between. Here are some important details:

- Shows **all networks that are currently blocked** by the Sentinel, with details about the event that got them blocked.
- **Release networks** by clicking the 'release' button, and choosing to release checked items, filtered items, or all. The 'Release checked' option will release all checked events on the current page. 'Release filtered' will release all events that meet your current keyword and/or date filter criteria. 'Release all' will quite literally release all blocked networks (obviously, be careful with that one).
- There are four **severity** levels: The first three are designated 1 through 3, with 3 being critical. The fourth level is reserved for the most critical alerts; we call these 'Flagged' alerts, and if there are any flagged alerts that you haven't reviewed, a notification banner will display in the upper right hand corner of the title bar. We take 'Flagged' alerts seriously – so should you.
- Events are clickable, showing **details about the attack**, such as source and destination IP and port, protocol, and packet detail. Blocked IPs are displayed in red, and the Protected Network is displayed in blue. The 'actions' button allows you to create a support ticket based on the specific alert, release the network if it's blocked, whitelist or blacklist a network, see other alerts of the same type, and click through to the Alert Detail page, which includes references for the specific alert type. The IP addresses within the event detail are also clickable, allowing you to view WHOIS information, CINS information, and a detailed summary of the IP address and its history on the Sentinel.
- You can **filter** by keyword, including partial words and IP addresses. Click the small down-facing arrow in the filter's text box to reveal a cheat sheet for some custom filters. You can also filter *out* keywords by adding a dash directly in front of the word. For example, to search for alerts that contain the word 'CINS' but do *not* contain the word 'rogue', you would enter *'CINS -rogue'*. Click the calendar icon to add a date filter; put the same date in both input boxes if you want to see a single day, or leave one of the date fields empty to get a range up to or starting from a given date.
- If **X-Forwarded-For (XFF)** recognition has been enabled, events that contain proxy information will display a small 'p' near the left-hand side of the screen.
- Click a column heading to sort by that column. Click it again to reverse the sort order. Any filter you have set will remain in place.
- The upper-right corner below the grey title bar always displays the total number of alerts, based on the current filter. If there is no filter, the number shown is the total number of networks currently blocked by the Sentinel.
- Results are paged, 50 items per page. The paging navigation appears at the bottom. Click the arrows to navigate to the first, last, previous and next page. Enter a page number in the input box and hit enter to go directly to a specific page.

- **Badges:** On the far right of every alert, there are 2 badges:
  - The **EPS** badge identifies an alert as 'Extrusion Protection'. EPS traffic can technically be inbound or outbound, but these signatures usually look for outbound traffic indicative of a botnet or malware infection within your LAN. These are usually worth your immediate attention, so we highlight them with this red badge.
  - The **REP** badge identifies reputation-based alerts. These alerts are based on the reputation of the offending IP address, not the content of the IP's communication with your network. Sorting this column lets you quickly identify which alerts are signature-based (No REP badge) and which alerts are reputation-based (blue REP badge).

Event Summary

Shows a **summary of every event that has ever happened on the Sentinel**, whether the network that tripped the event is still blocked or not.

- Click one of the prominent links below the page title to summarize by Attack Type, Protected IP Address, External IP Address, or – if XFF recognition has been enabled – X-Forwarded-For IP.
- Clicking the Attack Type text will take you to the **Event Activity** page, filtered for the corresponding summary event.
- The upper-right corner below the title bar always displays number of summary records, based on the current filter. If there is no filter, the number shown is the total of all activity on the Sentinel.
- **Badges:** There is one additional badge on this page that does not appear on Blocked Networks. The **AO** badge identifies events that correspond to Alert Only signatures, meaning that the Sentinel has logged this event for informational purposes, but this specific event did not get the offending IP blocked.

Event Activity

Shows **every event that's ever happened** on the Sentinel, whether the network that tripped the event is still blocked or not. Think of it as an **ad-hoc reporting tool** where you can track down any activity that has ever occurred on the Sentinel.

- The way events are displayed on the page, including the keyword and date filtering, is very similar to the Blocked Networks page, so please refer to that section for more details.
- The upper-right corner below the title bar always displays total number of alerts, based on the current filter. If there is no filter, the number shown is the total of all activity on the Sentinel.
- **Badges:** There is one additional badge on this page that does not appear on Blocked Networks. The **AO** badge identifies events that correspond to Alert Only signatures, meaning that the Sentinel has logged this event for informational purposes, but this specific event did not get the offending IP blocked. (It is possible that the IP may already be blocked for something else. Click the event, then choose 'IP Detail' from the IP's menu to find out more.)

Configuration

This is where you can configure options specific to your network environment.

Network Controls

Each of the Network Control options is managed the same way: You can add, modify, or delete as many individual entries as you'd like. But, once you've completed your edits, you ***must*** click the 'Commit Configuration Changes' button at the bottom of the page for your configuration changes to become active.

- **Protected Networks:** Network ranges protected by the Sentinel IPS. Any traffic destined to these networks that is deemed malicious by the Sentinel will be blocked.
- **Whitelisted Networks:** Trusted network ranges or IP addresses outside of the protected networks. The Sentinel will not block these networks for any reason. Their traffic is quite literally ignored by the Sentinel, and their activity does not show up in the Sentinel's reporting tools. Use whitelists judiciously – if the Sentinel is tripping false positive activity, there is usually another remedy before we resort to whitelisting.
- **Blacklisted Networks:** Ensures the specified network will never reach your protected network ranges. All traffic from these networks will be blocked immediately, and ignored. As such, blacklisted networks do not show up anywhere in the Sentinel's reporting tools.
- **Remote Administration:** Allows the specified network access to the Sentinel's web interface. Only networks listed here and in Protected Networks can access the web interface.
- **Remote DNS Servers:** Allows traffic to the specified network on port 53 (the standard port for DNS). If your network relies on external DNS servers for DNS resolution, enter them here. Note that malicious traffic detected on ports other than 53 will get the offending IP address blocked, even though it will always be allowed to communicate over port 53.
- **Block TTLs:** Specifies the time a blocked network remains on the Current Blocked Networks list. There is a default setting for all networks, but you can also add a setting for a specific network range.

System Controls

- System Settings and Tools
  - Displays the Sentinel's **current IP** address, netmask, and gateway settings, and its serial number.
  - You may switch between **Cloaking** mode and **Alert Only** mode. Cloaking mode is the default working mode for a Sentinel, and while a unit is in Cloaking mode it performs its core function of blocking malicious traffic. If you need to troubleshoot network issues and you suspect the Sentinel might be causing a problem, you can switch to Alert Only mode. The Sentinel will still record malicious activity but WILL NOT BLOCK ANY traffic for any reason.
  - The **interface settings** are displayed here, along with the NICs' current status. If all is well, both NICs will show as 'active'. In addition, if a NIC has auto-negotiated to its current setting, the page will show 'auto' after the setting description.

- The system **time zone** setting may be changed here. This setting is for display purposes only, and does not affect the systems core controls. That means if you'd like to review a report or activity page from the perspective of a different time zone, feel free to adjust this setting as often as you'd like. That can be handy when correlating event data across systems that span different time zones.

- Remote Logging
  - Allows the Sentinel to **log Alert data to a SEIM or remote syslog server**.
  - The setup is very straightforward, and **only requires the IP and port** of the remote server. You can also choose TCP or UDP; we recommend TCP, because TCP allows the Sentinel to hold the alert data in a queue in case communication to the remote server is lost temporarily. When communication is restored, the queued data is forwarded to the remote server, and there are no gaps in the timeline of the activity. Due to its stateless nature, UDP cannot queue data and makes no consideration for lost connections.
  - Please note that the IP address in the configuration **must be publicly routable**, since the Sentinel is typically installed in public IP space. Therefore, if your remote server or SEIM is located on the LAN with an internal IP address, you will have to configure your firewall or border device with a one-to-one NAT or port forward to route the alert data properly.
  - The current format of the exported data is:

    timestamp | src | src port | dst | dst port | severity | attack description

- Organizational Info
  - **Organization Name:** Enter your organization's name and the location of the Sentinel here. Be specific when describing the location; it helps us identify specific units more quickly, especially when companies have more than one Sentinel unit installed.
  - **Security Question/Answer:** If we are unsure of your identity for any reason, we will ask you this security question. This is not specific to each individual user, so make sure all users of the Sentinel will know the answer.
  - **Billing and Shipping Addresses:** Be sure to keep these addresses up to date.

- User Management
  - Shows **active users**. Click their username to **edit their account**.
  - Users are never deleted, only inactivated. If there are inactive users, a button will display next to the 'add a user' button that will allow you to show (and edit) the inactive users.
  - User's edit page: A user's **basic personal information**. A note about the 24/7 phone: Please give us a phone number where we can reach you even if your network is down. Standard office phone numbers – especially VOIP systems – can obviously prove to be unreachable during a network outage, so your cell phone is usually a good choice. You can choose to be texted or called after hours.
  - There are 5 **Access Levels (ACLs)**:

        - **Administrator:** Can perform every function on the user interface, including management of other users. Also has access to the Transaction History.
        - **Power User:** Can perform every function on the interface, except management of other users. Cannot view transaction history.
        - **CBNets User:** Can view reporting and can release blocked networks, but CANNOT change any other configuration settings like whitelists, mode, or time zone. Also cannot manage other users or view the transaction history.
        - **Reader:** Can view reporting and other activity, but cannot release networks, manage users, or change any configuration settings. Perfect for management-level employees that might be required to review information but should not be allowed to change any settings.
        - **Auditor:** Same as reader, but also has access to the Transaction History. As the name implies, perfect for an auditor that is required to review employee activity, but should not be allowed to configure the unit.
    - Contact Level
        - **Primary Contact:** If our monitoring system detects that the Sentinel is offline, we will contact this person as soon as possible by phone, based on their user profile preferences. If there are multiple Primary Contacts, we will attempt to contact them all.
        - **Alternate Contact:** If we cannot reach a Primary Contact, we will attempt to contact the Alternate. There can be multiple Alternate Contacts, as well.
        - If you want to be sure that you are never contacted for any reason, select **'None'**.
    - Active?
        - If this is checked, the user can access the Sentinel's interfaces. If this is unchecked, the user will be inactivated and unable to access the interfaces. To help keep audit trails and the Transaction History intact, users cannot be deleted. If you want to remove a user's access, simply inactivate him.

Reporting

All the reports default to specific time frame, but each can be customized to a different date range by using the **date filter** at the top of the page. Here is a brief overview of the reports available on the Sentinel:

- **Top Attacks:** Lists the top attack types and top offending IP addresses, so you can quickly find out which IPs and which types of attacks are affecting your network. Since these lists all link to more detailed reporting, this is a great starting point when researching a network issue.
- **Activity Summary:** The graphic shows all activity by day, and the summary table below it lists every attack type that hit the Sentinel for the given time period. Change the date range to a single day, and the chart will show hourly activity for that day.
- **Service Report:** A summary of everything on the Sentinel for the given time period, including some basic configuration settings, a log of user activity, and a list of the top attacks.

- **EPS Activity:** EPS activity is an indication that your network might have an infected machine on the inside. Since this can be an urgent issue, we provide the EPS Activity page as a simple way to keep an eye on these types of alerts. It is essentially the same functional page as the Event Activity page, only filtered specifically for EPS activity, so see the Event Activity section for more details.
- **Released IP Addresses:** Provides a complete history of all IP addresses that have been released from the Sentinel's list of blocked networks. The report defaults to showing releases that were user-generated, as is the case when a network is whitelisted or released directly from the Blocked Networks page. Clicking the 'Show TTL Releases' button will also show the automated releases that occur based on the Block TTL settings. The alert details are similar to the Blocked Networks and Event Activity pages, so see those sections for more information.
- **Port Detail:** This report summarizes destination protocol/port activity by volume and by unique IP address.
- **Email Scheduler:** Basic versions of the Top Attacks report, Activity Summary, and Service Report are available as regularly scheduled email reports. This is a global setting, so any administrator or power user can control the timing of the reports and their recipients.

Compliance

This section gives some examples of how the Sentinel can assist you with various compliance guidelines, such as GLBA, HIPAA, PCI, and others. It also provides a link to the Transaction History of the Sentinel, assuming you have administrator or auditor permissions.

Support

Provides a phone number to reach us anytime (972.991.5005), a list of available documentation regarding the Sentinel, and Support Ticket submission form. Contact us anytime, any way… we'd love to hear from you.

Detail Pages

Each event on the Sentinel can be broken down in to two core components: The attack type, and the IP addresses involved. These detail pages endeavor to give you all the information you need to analyze these items on one, simple page. You will come across these pages as you drill in to events on the interface:

IP Detail

This page shows all the information we know about the given IP address, and lets you act upon that information. On this page you will find:

- The IP's **country** of origin
- Whether the IP is **currently blocked** or not
- A summary of **alerts** related to this IP
- A summary of **configuration settings** related to this IP

- In the case of external IP addresses, a **timeline** of all events and configuration activities related to this IP
- In the case of external IP addresses, the page also lists all the **dropped packets** related to this IP.

Using the page's 'actions' button, you can:

- **Release** the IP from current blocked networks
- **Whitelist** or **blacklist** the IP
- See **WHOIS** and **CINS** information
- See **all activity** related to this IP on the Event Activity page.

Alert Detail

This page shows all the specifics of the given event, and lets you act upon that information. On this page you will find:

- The **attack type** and Sentinel-specific **alert number**
- The **severity** of the event
- EPS, Alert Only, and Reputation **badges**
- Source, destination, port, flow, protocol, and packet detail information
- **Reference links** specific to this type of alert, if available
- A detailed list of subsequent **dropped packets**.

Using the page's 'alert actions' button, you can:

- Create a **support ticket** specific to the given alert
- **Release** the offending IP related to this alert from the current blocked networks
- **Whitelist** or **blacklist** the offending IP
- View **all alerts** of this type on the Event Activity page.