




## SONICWALL SonicOS 7.1 Device Log User Guide

[Home](#) » [SONICWALL](#) » SONICWALL SonicOS 7.1 Device Log User Guide 



### SonicOS 7.1 Device Log Administration Guide

#### Contents

- [1 About SonicOS](#)
- [2 Working with SonicOS](#)
- [3 How to Use the SonicOS Administration Guides](#)
- [4 About Device](#)
- [5 Settings](#)
- [6 Filtering the Base Setup View](#)
- [7 Configuring the Logging and Alert Levels](#)
- [8 About Other Top Row Buttons](#)
- [9 About the Log Settings Base Setup Table](#)
- [10 Internet Protocol Flow Information Export \(IPFIX\) Column](#)
- [11 Configuring Event Attributes Globally](#)
- [12 Configuring Event Attributes Selectively](#)
- [13 Syslog](#)
- [14 Syslog Settings](#)
- [15 Automation](#)
- [16 Name Resolution](#)
- [17 Reports](#)
- [18 AWS](#)
- [19 SonicWall Support](#)
- [20 Documents / Resources](#)
  - [20.1 References](#)
- [21 Related Posts](#)

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on how to configure the device settings, capture all log activities, configure log files and report the logs on the Sonicwall security appliances

## Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- Policy Mode provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- Classic Mode is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

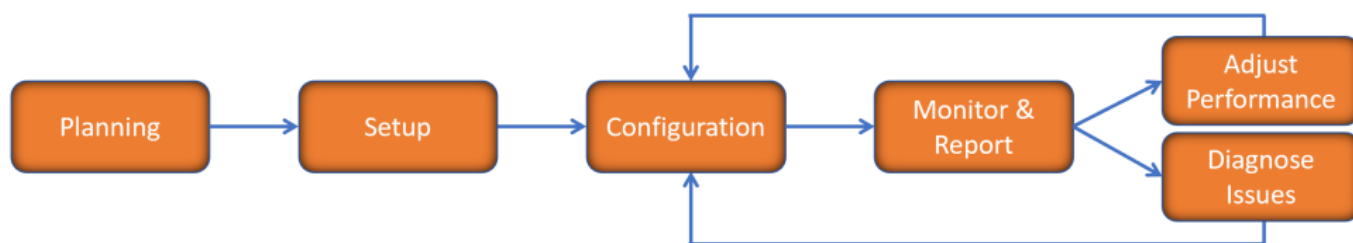
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPPS bandwidth issues; built-in SDWAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

1. SonicOS 7.1 API Reference Guide
2. SonicOS Command Line Interface Reference Guide

## SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

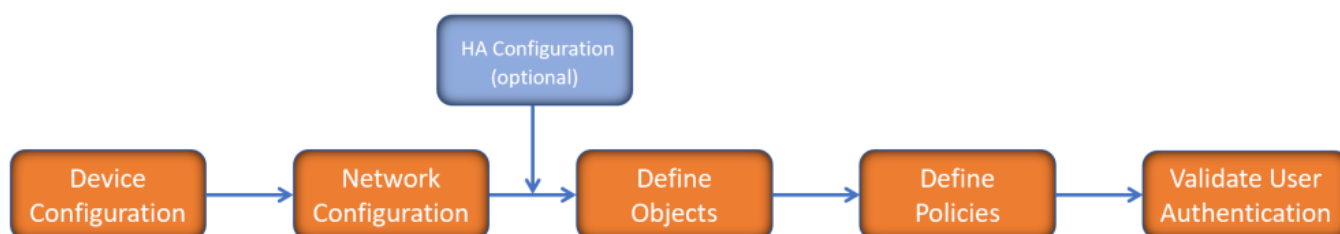


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your environment and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing product information and solutions. After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The Getting Started Guides for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the specific Administration Guide for a SonicOS feature for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

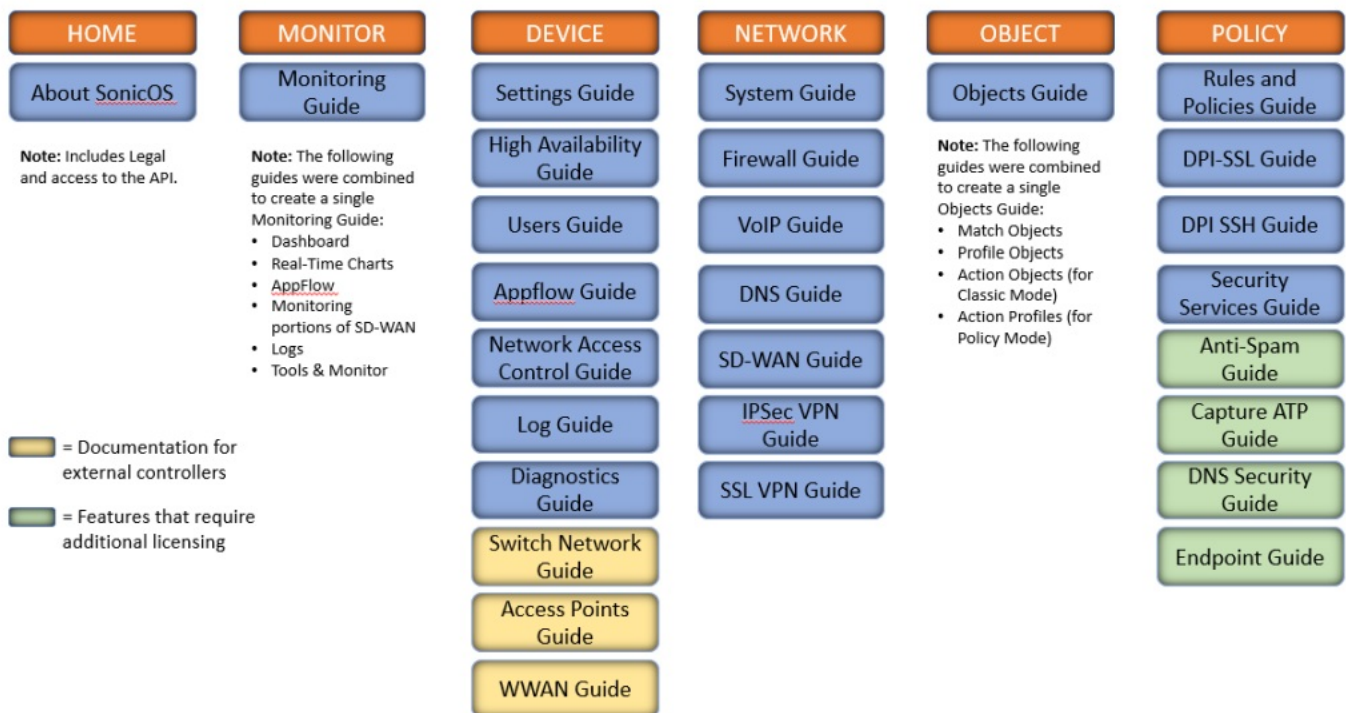


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

## How to Use the SonicOS Administration Guides

The SonicOS Administration Guide is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the SonicOS 7.1 Monitor Guide and the SonicOS 7.1 Objects Guide which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the <https://www.sonicwall.com/support/technical-documentation/>.

## Guide Conventions

These text conventions are used in this guide:



**NOTE:** A NOTE icon indicates supporting information.



**IMPORTANT:** An IMPORTANT icon indicates supporting information.



**TIP:** A TIP icon indicates helpful information.



**CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



**WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function   Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, NETWORK   System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page.
Code	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=<your serial number>, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004.
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

## About Device

SonicOS comes equipped with several features to configure Device. Basic Device information can be viewed in the Dashboard (navigate to HOME > Dashboard). The other Device configuration tools are grouped under the Device option as follows.

CATEGORY	COLOR	ID	PRIORITY	GUI	ALERT	SYSLOG	TRAP	IPFIX	EMAIL	EVENT COUNT
Anti-Spam	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Firewall	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7
Firewall Settings	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9063
High Availability	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Log	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	85
Multi-Instance	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Network	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	701523
Object	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
SD-WAN	<input checked="" type="checkbox"/>		debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3
Security Services	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	48
SSL VPN	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	24
System	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	76
Unified Policy Engine	<input checked="" type="checkbox"/>		inform	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1623
Users	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	51
VoIP	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
VPN	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
WAN Acceleration	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Wireless	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
WWAN Modem	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0

- Settings – To manage the Administration settings.
- High Availability – To view the status, configure, support licenses and to monitoring.
- Users – To view status of local and guest users.
- AppFlow – To configure Flow Reporting and AppFlow Agent.
- Log – To captures all log activities, configure log files and report the logs.
- Diagnostics – To configure system diagnostics.

## Device Log Introduction

The Device option is a collection of setup options you can use to configure the device settings, capture all log

activities, configure log files and report the logs.

**SONICWALL** NSv 870 HOME MONITOR **DEVICE** NETWORK OBJECT POLICY

00401039D18F / Device / Log / Settings

Accept Cancel Filter Logging Level: **Debug** Alert Level: **Warning** View Logs

CATEGORY	COLOR	ID	PRIORITY	GUI	ALERT
▶ Anti-Spam	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Firewall	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Firewall Settings	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ High Availability	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Log	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Multi-Instance	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
▶ Network	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Object	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input type="checkbox"/>
▶ SD-WAN	<input checked="" type="checkbox"/>	...	debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Security Services	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ SSL VPN	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input type="checkbox"/>
▶ System	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Unified Policy Engine	<input checked="" type="checkbox"/>	...	inform	<input type="checkbox"/>	<input type="checkbox"/>
▶ Users	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ VoIP	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input type="checkbox"/>
▶ VPN	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ WAN Acceleration	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
▶ Wireless	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
▶ WWAN Modem	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The commands on the left shows differ kinds of options. Once an option is selected, you can view different aspects of the data by selecting the different tabs. More information on each of the options are provided in the following chapters:

## Settings

This section provides configuration tasks to enable you to categorize and customize the logging functions on your SonicWall security appliance for troubleshooting and diagnostics.

**SONICWALL** TZ 470 HOME MONITOR **DEVICE** NETWORK OBJECT POLICY

2CB8ED69530C / Device / Log / Settings

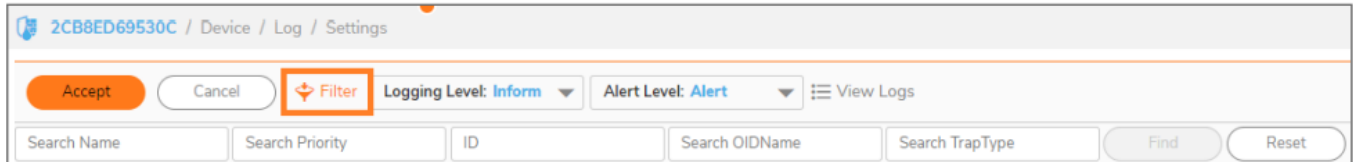
Accept Cancel Filter Logging Level: **Inform** Alert Level: **Alert** View Logs

CATEGORY	COLOR	ID	PRIORITY	GUI	ALERT	SYSLOG	TRAP	SMTP	EMAIL	EVENT COUNT
▶ Anti-Spam	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Firewall	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Firewall Settings	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	518
▶ High Availability	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Log	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	13
▶ Multi-Instance	<input type="checkbox"/>	...	mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Network	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1305936
▶ Object	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ SD-WAN	<input checked="" type="checkbox"/>	...	debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3
▶ Security Services	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	23694
▶ SSL VPN	<input type="checkbox"/>	...	mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	40

The Device > Log > Settings page displays logging settings in a series of columns and allows you to configure the logging and alert levels, edit attributes of all categories, groups, and reset all event counts. You can filter the entries to limit the data display to only those events of interest. You can select storage options on appliances with built-in or flexible storage components, and you can import and save logging templates.

## Filtering the Base Setup View

You can filter the log data by using the Filter icon on the Device > Log > Settings page to filter at the category, group, or event level. This provides a way to filter the display of Log > Settings to make it easier to view settings of selected events. The Filter View in this context only allows “Name, Priority, ID, OIDName and TrapType.” Enter the Name, Priority, ID, OIDName or TrapType and click Find to filter the log data. Click Reset to clear the filter applied.

The screenshot shows the top navigation bar of the SonicOS interface. The breadcrumb trail is "2CB8ED69530C / Device / Log / Settings". Below the breadcrumb, there are buttons for "Accept", "Cancel", and a "Filter" button with a magnifying glass icon, which is highlighted with an orange box. To the right of the Filter button are dropdown menus for "Logging Level: Inform" and "Alert Level: Alert", followed by a "View Logs" button. Below these elements is a search bar with fields for "Search Name", "Search Priority", "ID", "Search OIDName", and "Search TrapType", and "Find" and "Reset" buttons.

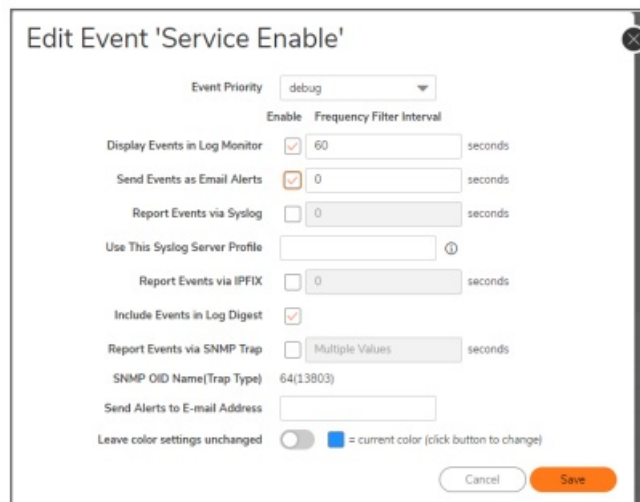
Log data is displayed on the Monitor > Logs > System Logs page that has its own Filter View that is more granular. You can navigate to the Logs > System Logs page quickly by clicking View Logs in the top row of the Log > Settings page. For more information, see SonicOS 7.1 Monitor Guide.

## Configuring the Logging and Alert Levels

This section provides information on configuring the level of priority of log messages that are captured, and the corresponding alert messages that are sent through email for notification.

Alert emails are sent when enabled and an email address is configured. Specifically:

- Select the Enable option Send Events as Email Alerts in the Edit Log Event dialog launched from the table on the Log > Settings page.

The screenshot shows the "Edit Event 'Service Enable'" dialog box. It has a title bar with a close button. Inside, there is a dropdown for "Event Priority" set to "debug". Below this is a table with columns "Enable" and "Frequency Filter Interval". The rows are: "Display Events in Log Monitor" (checked, 60 seconds), "Send Events as Email Alerts" (checked, 0 seconds), "Report Events via Syslog" (unchecked, 0 seconds), "Use This Syslog Server Profile" (empty field with an info icon), "Report Events via IPFIX" (unchecked, 0 seconds), "Include Events in Log Digest" (checked), "Report Events via SNMP Trap" (unchecked, Multiple Values seconds), "SNMP OID Name(Trap Type)" (64(13803)), and "Send Alerts to E-mail Address" (empty field). At the bottom, there is a toggle for "Leave color settings unchanged" (currently off) and a "Save" button.

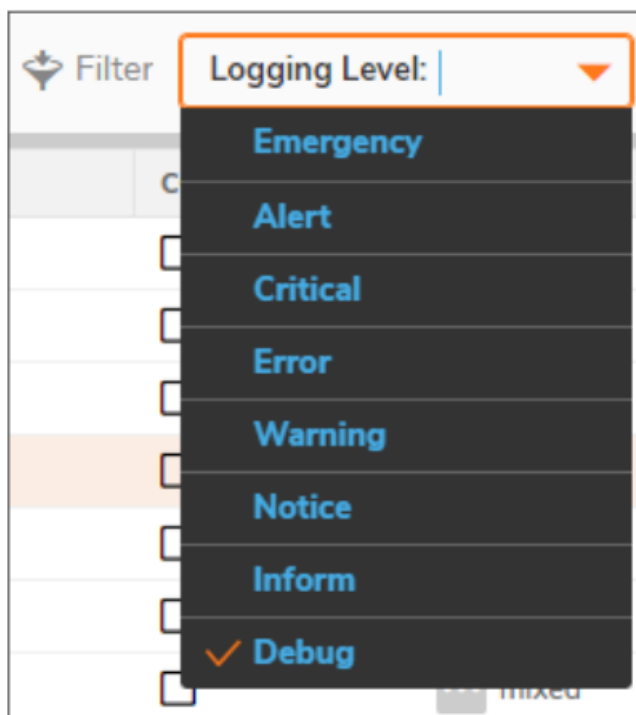
- There is an email address configured in Send Alerts to E-mail Address in the Log > Automation page or in one of the following Edit dialogs launched from the table on Log > Settings page.
- Edit Log Category dialog
- Edit Log Group dialog
- Edit Log Event dialog

## About SonicOS

The Logging Level provides a way to use the Event Priority setting of the event to filter for log generation. Events with equal or greater priority are logged. Events with a lower priority are not logged. This enables you to filter out lower-level priorities to prevent them from being logged. This Logging Level filtering is done at the beginning of logging the event, before any other filtering settings are applied. The Logging Level filtering affects which logs are actually stored in the Log database (and storage), unlike the Filter icon that only affects the display of those logs.



**i** TIP: While the Event Priority for each event has a factory default value, the Edit dialogs allow the Event Priority to be customized as needed on the Category level, Group level, or individual Event level. By changing the Event Priority for selected events, administrators can include events that are otherwise filtered out because of the Logging Level setting. For example, a factory default Debug event can be set to have an Event Priority of Warning so that it is included in the logs when Logging Level is set to Warning.



On the Log > Settings page, you can set the baseline logging level to be displayed on the Monitor > Logs > System Logs page. The following logging levels are available for selection, from highest to lowest:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Inform
- Debug

The default level is Inform.

To set the logging level:

1. Navigate to the Log > Settings page.
2. From the Logging Level drop-down menu, select the logging level you want.

All events with Event Priority equal to or higher than the selected entry are logged. For example, if you select Error as the Logging Level, all messages with Event Priority of Error, Critical, Alert, and Emergency are logged.

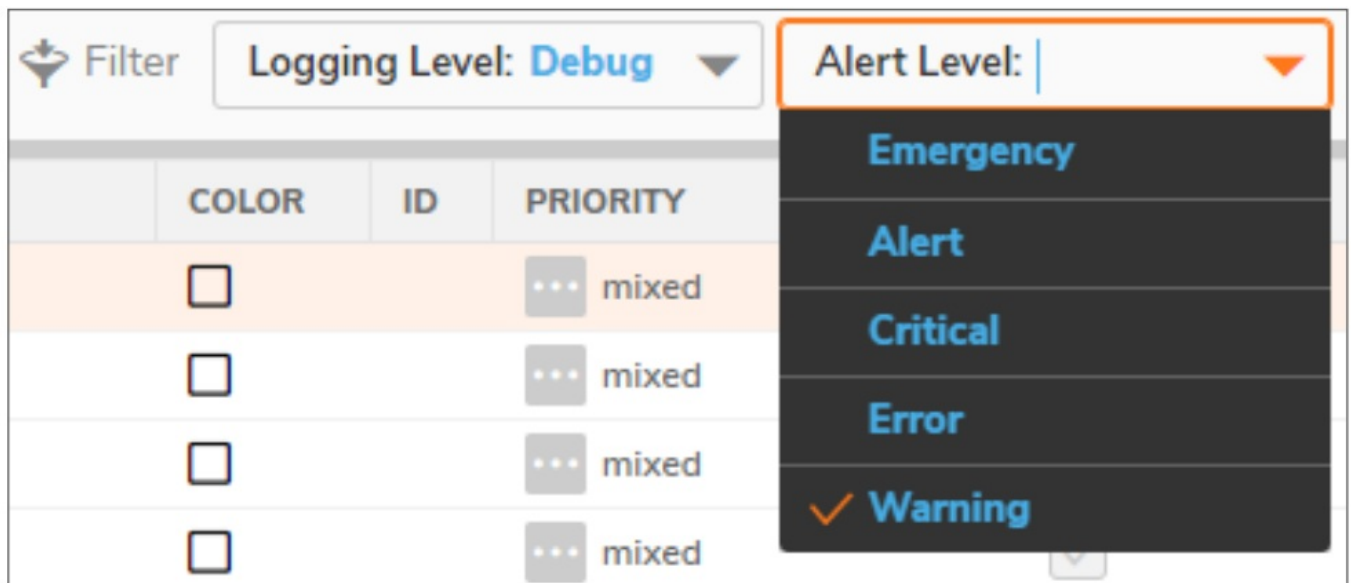
**i** NOTE: To display all events, select Debug as the logging level.

## Setting the Alert Level

The Alert Level provides a way to use the Event Priority setting of the event to filter for email alerts generation. It is assumed that the event has already been included after applying the Logging Level filter and after applying the Frequency Filter Interval configured for the Send Events as E-mail Alerts option in the Edit dialogs. For Alert Level filtering, only events with an Event Priority of Warning or higher are included.

**i** TIP: While the Event Priority for each event has a factory default value, the Edit dialogs allow the Event Priority to be customized as needed on the Category level, Group level, or individual Event level. By changing the Event Priority for selected events, administrators can include events that are otherwise filtered out because of the Logging Level setting. For example, a factory default Debug event can be set to have an Event Priority of Warning so that it is included in the logs when Logging Level is set to Warning.

Email alerts are sent to the email address configured in Send Alerts to E-mail Address in the Log > Automation page or, if set, configured in one of the Edit dialogs launched from the table on the Log > Settings page. Events with an alert level equal to or greater than the configured Alert Level are sent to the specified email address. No email alerts are sent for events with a lower alert level. This enables you to filter out lower-level email alerts to reduce the actual emails transmitted.



The following alert levels are available for selection:

- Emergency
- Alert
- Critical
- Error
- Warning

The default value is Alert.

To set the alert level:

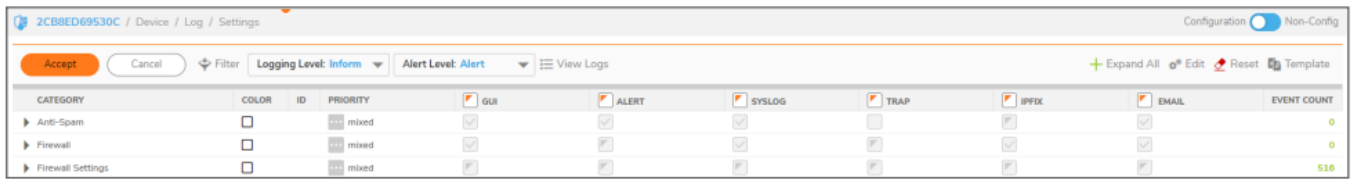
1. Navigate to the Log > Settings page.
2. From the Alert Level drop-down menu, select the alert level you want.

All events with Event Priority equal to or higher than the selected Alert Level are also emailed. For example, if you select Error as the Alert Level, all messages all messages with Event Priority of Error, Critical, Alert, and Emergency are emailed.

**i** TIP: To email alerts for events of all alert levels, select Warning as the Alert Level.

## About Other Top Row Buttons

The Logging Level and Alert Level configurations are described previously. This section provides a summary of the other buttons that appear above the table on the Device > Log > Settings page.



2CB8ED69530C / Device / Log / Settings

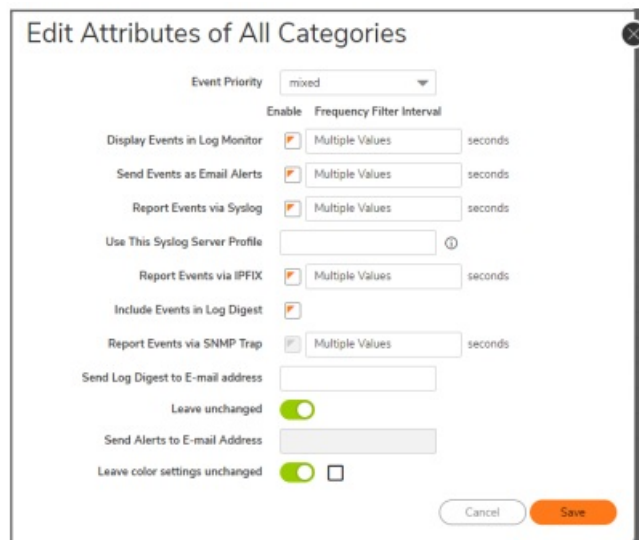
Configuration ☒ Non-Config

Accept Cancel Filter Logging Level: Inform Alert Level: Alert View Logs Expand All Edit Reset Template

CATEGORY	COLOR	ID	PRIORITY	GUI	ALERT	SYSLOG	TRAP	IPFIX	EMAIL	EVENT COUNT
Anti-Spam	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Firewall	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Firewall Settings	<input type="checkbox"/>		mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	536

### Edit Attributes of All Categories

Clicking the Edit All Categories Attributes button above the table launches the Edit Attributes of All Categories dialog. This dialog enables you to set the attributes for all events in all categories and groups at once.



Event Priority: mixed

Enable Frequency Filter Interval

Display Events in Log Monitor ☒ Multiple Values seconds

Send Events as Email Alerts ☒ Multiple Values seconds

Report Events via Syslog ☒ Multiple Values seconds

Use This Syslog Server Profile

Report Events via IPFIX ☒ Multiple Values seconds

Include Events in Log Digest ☐

Report Events via SNMP Trap ☒ Multiple Values seconds

Send Log Digest to E-mail address

Leave unchanged ☒

Send Alerts to E-mail Address

Leave color settings unchanged ☒

Cancel Save

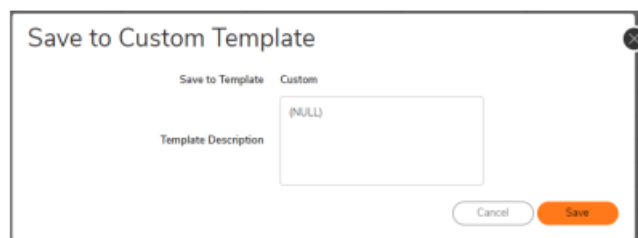
For information about this procedure, refer to Configuring Event Attributes Globally.

### Reset All Event Counts

Click the Reset button to set all the event counters to 0.

### Save Template

Save Template displays the Save to Custom Template pop-up dialog so you can export the current configured Log Settings to the Custom template. The dialog also lets you enter a description for the Custom template.



Save to Template Custom

Template Description (NULL)

Cancel Save

Only the Custom template can be modified and saved, and there is only one custom template. Each time the custom template is saved, the old custom template is overwritten.

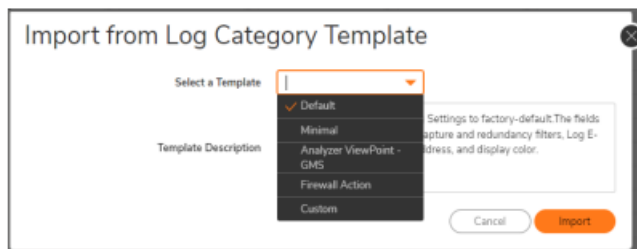
### Import Template

Clicking on the Import From Template button displays the Import from Log Category Template dialog that allows you to select and import one of these templates:

- Default

- Minimal
- Analyzer / Viewpoint / GMS
- Firewall Action
- Custom

You can select Custom if you previously saved a template using Save As Custom. If there is no user template saved, Custom option cannot be selected.



**CAUTION:** The imported template overwrites individual settings. Normally, production environments would not set all Categories/Groups/Events to have exactly the same settings. Before doing this, be sure to save your current configuration using the Save Template option, so that the previous settings can be restored when a mistake is made by using Import Template > Custom.

Also, factory default settings can be restored using Import Template > Default.

**NOTE:** The Default, Minimal, and Analyzer/Viewpoint/GMS templates are default templates defined in SonicOS.

### Default Template

The Default template restores all log event settings to the SonicOS default values for each of these log fields:

- Event Priority
- Display Events in Log Monitor
- Send Events as E-mail Alerts
- Report Events through Syslog
- Include Events in Log Digest
- Frequency Filter Interval
- Send Log Digest to E-mail Address
- Send Alerts to E-mail Address
- Show Events using Color

### Minimal Template

The Minimal template keeps the generated logs at a minimum level, while still providing sufficient information about the most important events on the firewall. The minimal template modifies the capture filters to allow only high-priority events to be logged. Most non-critical events are filtered out. The capture filters are modified for these fields: GUI, Alert, Syslog, and Email.

**NOTE:** Only the capture filters are modified; the Frequency Filter Interval settings are left as is.

### Analyzer/ViewPoint/GMS Template

The Analyzer/Viewpoint/GMS template ensures that the firewall works well with Reporting Software server settings (Analyzer, Viewpoint, and/or GMS server). All related events are configured to meet the server requirements.

All configurations are limited to the Report Events via Syslog option and its associated Frequency Filter Interval. Events critical to the reporting function of Analyzer, Viewpoint, and GMS has these fields set to the recommended

factory-default values:

- Report Events via Syslog
- Frequency Filter Interval for Syslog

## Firewall Action Template

The Firewall Action template is based on the Analyzer/ViewPoint/GMS Template. In addition to the settings that the Analyzer/Viewpoint/GMS Template provides, it enables logs that report dropped packets.

## Custom Template

The Custom template is created by clicking Save Template. Each time you click Save Template, the previous Custom template is overwritten. Importing it brings back the saved settings.

## View Logs

The View Logs button in the top row takes you to the Monitor > Logs > System Logs page where you can view the log data. For more information about logs, refer to SonicOS 7.1 Monitor Guide.

## About the Log Settings Base Setup Table

Following are columns present in the Log Settings page.

### Category Column

The Category column of the Log Settings table has three levels:

- Category, first and highest level of the tree structure
- Group, the second level
- Event, the third level

Clicking the triangle icon to the left of the category or group name expands or collapses the category or group contents:

CATEGORY	COLOR	ID	PRIORITY	GUI	ALERT	SYSLOG	TRAP	IPFIX	EMAIL	EVENT COUNT
▼ Anti-Spam <b>1st Level</b>			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ E-mail			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ General			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ GRID			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Probe			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▼ Firewall			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Application Firewall <b>2nd Level</b>			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▼ Security Policy			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Rule Added		440	inform	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Rule Modified		441	inform	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Rule Deleted		442	inform	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Source IP Connection Limit		646	warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Destination IP Connection Limit		647	warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Source Connection Status		734	warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Destination Connection Status		735	warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▼ Firewall Settings			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	516
▶ Advanced <b>2nd Level</b>			mixed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Checksum Enforcement			notice	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ Flood Protection			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ PTP			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Multicast			mixed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	516
▶ SSL Control			inform	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

### Color Column

The Color column shows the color with which the event is highlighted in the Monitor > Logs > System Logs. To

change the color of the event, click the Edit icon for the event.

### ID Column

The ID column shows the ID number of the event. The ID for a particular message is listed in the SonicOS Log Events Reference Guide.

The ID number of the event is the same value used in Syslog as the m= message ID and can also be found in the Event ID column of Log Event Message Index table in the SonicOS Log Events Reference Guide.



**NOTE:** The ID number is only displayed on the event level that can be either second or third level.

### Priority Column



**CAUTION:** Changing the Event Priority could have serious consequences. Changing the Event Priority on the Group or Category level also changes all Events under that Group or Category to the same Event Priority value. Modifying the Event Priority affects the Syslog output for the tag “pri=” as well as how the event is treated when performing filtering by Logging Level or Alert Level.

Setting the Event Priority to a level that is lower than the Logging Level causes those events to be filtered out. Also, as SonicWall GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages must have a minimum Event Priority of Inform.

The Priority column shows the severity or priority of a category, group, or event. For events, a drop-down menu lists the selectable priorities. For categories and groups, the priorities are listed in the dialog when you click Configure at the end of the row.

The available priorities are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Inform
- Debug

### GUI Column

The GUI column indicates whether this item is displayed in the Monitor > Logs > System Logs. The checkbox displayed for an Event in this column corresponds to the Enable checkbox setting for the Display Events in Log Monitor option in the Edit Log Event dialog.

Display of categories and groups is shown with a To show or hide indicator. To change the display for:

- An event, select or clear the checkbox in the column.
- Categories and groups, click the Edit icon in the column to display the Edit Log Category or Edit Log Group dialog.

### Alert Column

The Alert column indicates whether an Alert message is sent for this event, group, or category. The checkbox displayed for an Event in this column corresponds to the Enable checkbox setting for the Send Events as Email Alerts option in the Edit Log Event dialog.

The checkbox or indicator for Alert applies to both sending of an email per-event and to the generation of an

SNMP Trap (if SNMP configuration is enabled). For E-mail Alerts, the E-mail Address is either the global value set in the Send Alerts to E-mail Address field in the Device > Log > Automation > Email Settings page or the custom address configured in the Send Alerts to E-mail Address field in one of the Edit dialogs launched from the table on the Log > Settings page.

Whether the message is sent is shown with a To show or hide indicator. To change whether the Alert message is sent for:

- An event, select or clear the checkbox in the column.
- Categories and groups, click the Edit icon in the column to display the Edit Log Category or Edit LogGroup dialog.

### **Syslog Column**

The Syslog column indicates whether the event, group, or category is sent to a Syslog server. The checkbox displayed for an Event in this column corresponds to the Enable checkbox setting for the Report Events via Syslog option in the Edit Log Event dialog.

Whether the event, group, or category is sent is shown with a To show or hide indicator. To change whether the event, group, or category is sent for:

- An event, select or clear the checkbox in the column.
- Categories or groups, click the Edit icon in the column to display the Edit Log Category or Edit Log Group dialog.

### **Internet Protocol Flow Information Export (IPFIX) Column**

The IPFIX column indicates whether IPFIX is enabled for log events. The checkbox displayed for an Event in this column corresponds to the Enable checkbox setting for the Report Events via IPFIX option in the Edit Log Event dialog.

System logs can be sent to an external server through IPFIX packets and then saved into the database on the disk. The logs only include the ones reported without connection cache.

Whether the event, group, or category has IPFIX enabled is shown with a To show or hide indicator. To enable/disable IPFIX for:

- An event, select or deselect the checkbox in the column.
- Categories or groups, click the Edit icon in the column to display the Edit Log Category or Edit Log Group dialog.

### **Email Column**

The Email column indicates whether the log is emailed to the configured address. The checkbox displayed for an Event in this column corresponds to the Enable checkbox setting for the Include Events in Log Digest option in the Edit Log Event dialog. The Log Digest is further configured in the Device > Log > Automation > Email Settings page in the E-mail Log Automation section, in the Send Log to E-mail Address and Send Log (Daily, Weekly, When Full) options.

For events, these checkboxes are configurable in the column. For categories or groups, Email is configured in the Edit Log Group or Edit Log Category dialogs that appear when you click Edit at the end of the row.

### **Event Count Column**

The Event Count column shows the count of events by:

- Event level — The number of times that this event has occurred.
- Group level — The total events that occurred within the group.

- Category level — The total events that occurred within the category.

By hovering your mouse over an event count, a pop-up message displays the count of events dropped for these reasons:

EMAIL	EVENT COUNT	
		0
<b>Dropped by Reason:</b>		
Overflow	0	13
GUI Filter	0	0
Alert Filter	0	0
Syslog Filter	0	12
Trap Filter	0	0
IPFIX Filter	0	0
E-mail filter	0	0
Priority	0	1
Syslog Event Rate	0	0
Syslog Data Rate	0	0

- Overflow – count of events dropped because they cannot be enqueued for logging.
- GUI Filter – count of events dropped because the checkbox for Display Events in Log Monitor is disabled, or, if enabled, the event was dropped because of GUI Frequency Filter Interval.
- Alert Filter – count of events dropped because the checkbox for Send Events as E-mail Alerts is disabled, or, if enabled, the event was dropped because of Alert Frequency Filter Interval.
- Syslog Filter – count of events dropped because the checkbox for Report Events via Syslog is disabled, or, if enabled, the event was dropped because of Syslog Frequency Filter Interval.
- Trap Filter – count of events dropped because the checkbox for Report Events via SNMP Trap is disabled, or, if enabled, the event was dropped because of Trap Frequency Filter Interval.
- IPFIX Filter – count of events dropped because the checkbox for Report Events via IPFIX is disabled, or, if enabled, the event was dropped because of IPFIX Frequency Filter Interval.
- E-mail Filter – count of events dropped because the checkbox for Include Events in Log Digest is disabled, or, if enabled, the event was dropped because of E-mail Frequency Filter Interval.
- Priority – count of events dropped because the Event Priority was excluded from Logging Level.
- Syslog Event Rate – applies only to Syslogs dropped when Event Rate Limiting is enabled in the Device > Log > Syslog page, and Maximum Events Per Second exceeded the configured threshold.
- Syslog Data Rate – applies only to Syslogs dropped when Data Rate Limiting is enabled in the Log > Syslog page, and Maximum Bytes Per Second exceeded the configured threshold.

### Edit and Reset Count Icons

The Edit and Reset Event Count icons appear at the end of each row.



The Edit icon launches the Edit Log Event, Edit Log Group, or Edit Log Category dialog.



You can configure all of the attributes for an event, group, or category.



The Reset Event Count icon resets the event counter for an event, a group, or a category, and the event counters of higher levels are recalculated. To reset all counters, use Reset Event Count above the table on the Device > Log > Settings page, as described in Reset All Event Counts.

## Configuring Event Attributes Globally



**NOTE:** For information about configuring event attributes selectively, see Configuring Event Attributes Selectively.

Clicking the Edit All Category Attributes icon above the table launches the Edit Attributes of All Categories dialog. This dialog enables you to set the attributes for all events in all categories and groups at once.

These global attributes can be modified:

- Event Priority
- Inclusion of events in Log Monitor, Email, and Syslog
- Frequency Filter Interval
- Email settings
- Font color when displayed in Log Monitor

One practical use of this global setting is to force ALL events to use the same Syslog Server Profile (GMS uses Profile 0 only), send Log Digest to the same E-mail Address, and send Alerts to the same E-mail Address.

To edit the Category attributes globally:

1. Navigate to the Device > Logs > Settings page.
2. Click the Edit All Category Attributes icon. The Edit Attributes of All Categories pop-up dialog appears.



**NOTE:** Enable is solid green when all categories, groups, and/or events are enabled, white when all are disabled, and semi-solid when they are mixed (some enabled, some disabled).

As this configuration is for all categories, you have to explicitly set the option to “all enabled” by clicking the icon until it is solid green, or to set the option to “all disabled” by clicking the icon until it is white. To configure a single event to be different from the rest of its group or category, you must go into the individual event setting configuration. If you do this, the icon is semi-solid.

When the fields display Multiple Values, different values have been specified for one or more category, group, or event. To view the individual settings, refer to Configuring Event Attributes Selectively. To change the setting from Multiple Values into one value for all categories, groups, or events while in the Edit Attributes of All Categories dialog, verify that the option was enabled so the field can be accessed for entering the new value. If the option is disabled, the field is dimmed and inaccessible.



**CAUTION:** The changes are saved and overwrite individual settings. Normally, production environments would not set all Categories/Groups/Events to have exactly the same settings.

Before doing this, be sure to save your current configuration using the Save Template option, so that the previous settings can be restored if a mistake is made by using Import Template > Custom. Also, factory default settings can be restored using Import Template > Default.

3. From the Event Priority drop-down menu, select the priority that you want.



**CAUTION:** Changing the Event Priority globally uses the same value for all Events. Modifying the Event Priority affects the Syslog output for the tag “pri=” as well as how the event is treated when performing filtering by Logging Level or Alert Level. Setting the Event Priority to a level that is lower than the Logging Level causes those events to be filtered out. Also, as GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages must have a minimum Event Priority of Inform.



**TIP:** The following Frequency Filter Interval fields enable you to specify how many events of the same Event ID to log per time interval. Note that having the same Event ID does not mean that the event is a duplicate because the message itself might contain different information such as source/destination IP addresses, and so on. The filtering is done based on Event ID only. The range for these intervals is 0 to 86400 seconds.



**TIP:** The different options are independent of each other, and you can enable any combination of them and set different frequencies of generation for them. For example, you might want an event message emailed to you, but it is not shown in the Monitor > Logs > System Logs page. When GMS is enabled, however, care must be taken when modifying event attributes so events used to generate reports are not incorrectly filtered out. Explicit modification of individual events are saved even if used for GMS. Before making any changes, save current Log settings using Save Template.

This way, should a mistake be made, the previous settings can be restored using Import Template > Custom. As a last resort, the GMS settings can be restored using Import Template > Analyzer/Viewpoint/GMS.

4. If you want to display the log events in the Monitor > Logs > System Logs page, select the Enable icon for the Display Events in Log Monitor option.
  - In the Frequency Filter Interval field for Display Events in Log Monitor, enter the number of seconds that should elapse before allowing the same event to be logged and displayed again when that event occurs one after the other. The range is 0 to 86400.

For example, if you set this value to 60 seconds, then when the event Connection Closed first happens at 1:15 p.m., the next Connection Closed event to be displayed must occur at least 60 seconds after the first one. Any Connection Closed event occurring within the 60 seconds interval is not displayed.
5. If you want to send events as E-mail Alerts, select the Enable icon for the Send Events as E-mail Alerts option.
  - In the Frequency Filter Interval field for Send Events as E-mail Alerts, enter the number of seconds that should elapse before allowing the same email event to be sent when that event occurs one after the other. The range is 0 to 86400.

For example, if you set this value to 60 seconds, then when an E-mail Alerts first happens at 1:15 p.m., the next E-mail Alerts for the same event is not sent until 60 seconds after the first one.


Alerts for the same event occurring within the 60 seconds interval are not emailed.
6. If you want to report events through Syslog, select the Enable icon for the Report Events via Syslog option.
  - In the Frequency Filter Interval field for Report Events via Syslog, enter the number of seconds that should

elapse before allowing the same Syslog messages to be sent when that event occurs one after the other. The range is 0 to 86400.


For example, if you set this value to 60 seconds, then when a Syslog message is first reported at 1:15 p.m., the next Syslog message for the same event is not sent until 60 seconds after the first one. Syslog messages for the same event occurring within the 60-second interval are not sent.

7. To send the Syslogs to a particular Syslog server group, enter the group's ID in the Use this Syslog Server Profile field. The default is 0.
8. If you want to report events through IPFIX, select the Enable icon for the Report Events via IPFIX option.
  - In the Frequency Filter Interval field for Report Events via IPFIX, enter the number of seconds that should elapse before allowing the same events to be reported through IPFIX when events occur one after the other. The range is 0 to 86400.


For example, if you set this value to 60 seconds, then when an event reported through IPFIX first happens at 1:15 p.m., the next report for the same event is not sent until 60 seconds after the first one. Reports to IPFIX for the same event occurring within the 60 seconds interval are not sent.
9. If you want to include the events in the Log Digest, select the Enable icon for the Include Events in Log Digest option. The Log Digest is a chronological collation of events.
10. If you enabled Include Events in Log Digest, do one of the following for Send Log Digest to E-mail Address:
  - If you want to use the same email address that is entered in the Log > Automation page even when you change other values in this dialog, select Leave Unchanged. This option is enabled by default.


 NOTE: If this option is enabled, it is important to verify the email address configured in the Send Log Digest to Email Address field is correct.

  - To change the email address, clear the Leave unchanged option and enter a new address in the now-active field.

 TIP: An email alert is one email sent for each event occurrence as soon as that event has occurred. A Log Digest, on the other hand, is a chronological collation of events sent as a single email in digest format. Because it is a summation of events, the event information time period is a mix of older and newer events.
11. If you want to receive alerts through email based on the global settings in this dialog, do one of the following for Send Alerts to E-mail Address:
  - If you want to use the same email address that is entered in the Log > Automation page even when you change other values in this dialog, select Leave color settings unchanged. This option is enabled by default.
  - To change the email address, clear the Leave color settings unchanged option and enter a new address in the now-active field.
12. Click Save.

## Configuring Event Attributes Selectively

 NOTE: For how to configure event attributes globally, see Configuring Event Attributes Globally. On the Log > Settings page, the columns show the main event attributes that can be configured on different levels: category, group, or per event.

 NOTE: The Edit Log pop-up dialogs might look slightly similar, but the effect of each varies in scope.

- Edit Log Category dialog modifies settings for a category and all groups that belong to the same category and, consequently, all events in that category.

- Edit Log Group dialog modifies settings for a group and all events that belong to that group.
- Edit Log Event dialog modifies settings for one specific event.

**i NOTE:** Enable for the columns is green when all are enabled, white when all are disabled, and semi-solid when they are mixed (some enabled, some disabled).

As this configuration is for all categories, you have to explicitly set the option to “all enabled” by clicking the icon until it is solid green, or to set the option to “all disabled” by clicking the icon until it is white. To configure a single category, group, or event to be different, you must go into the individual dialog or event setting. If you do this, the icon is semi-solid.

You can enable or disable a column. In the rows for categories and groups, the enable indicators are gray (enabled, disabled, and mixed) and cannot be changed except through the Edit Log Category or Edit Log Group dialogs.

The rows for events contain checkboxes for enabling (✓) or disabling (✗) the event instead of indicators.

### Configuring Event Attributes by Category

Any changes done at the category level apply to all groups and all events within the selected category. To set the Event Attributes by category level:

1. In the Log > Settings page, click the Edit icon in the right-most column of the row with the category you want to edit. The Edit Log Category dialog for that category is displayed.

**Edit Category 'Anti-Spam'**

Event Priority: mixed

	Enable	Frequency Filter Interval
Display Events in Log Monitor	<input checked="" type="checkbox"/>	Multiple Values seconds
Send Events as Email Alerts	<input checked="" type="checkbox"/>	0 seconds
Report Events via Syslog	<input checked="" type="checkbox"/>	Multiple Values seconds
Use This Syslog Server Profile		
Report Events via IPFIX	<input checked="" type="checkbox"/>	Multiple Values seconds
Include Events in Log Digest	<input checked="" type="checkbox"/>	
Report Events via SNMP Trap	<input type="checkbox"/>	Multiple Values seconds
Send Log Digest to E-mail address		
Leave unchanged	<input type="checkbox"/>	
Send Alerts to E-mail Address		
Leave color settings unchanged	<input checked="" type="checkbox"/>	

Cancel Save

2. Follow the steps in Configuring Event Attributes Globally.

### Configuring Event Attributes by Group

Setting the Event Attributes by group level allows the modification of settings on a smaller scale within a selected category. Any changes done to the group apply to all events that belong only to the selected group.

To set the Event Attributes by group level:

1. In the Log > Settings page, click the arrow on the left to expand the category that contains the group you want to edit.
2. Click the Edit icon in the right-most column of the row with the group you want to edit. The Edit Log Group dialog for that group is displayed.

Edit Group 'E-mail'

Event Priority

mixed

Enable

Frequency Filter Interval

Display Events in Log Monitor

☒

60

seconds

Send Events as Email Alerts

☒

0

seconds

Report Events via Syslog

☒

0

seconds

Use This Syslog Server Profile

Report Events via IPFIX

☒

0

seconds

Include Events in Log Digest

☒

Report Events via SNMP Trap

☐

Multiple Values

seconds

Leave unchanged

☐

Send Alerts to E-mail Address

Leave color settings unchanged

☒

☐

Cancel

Save

3. Follow the steps in [Configuring Event Attributes Globally](#).

## Configuring Event Attributes by Event

The most granular level, the event level, allows the Event Attributes columns to be directly modified by expanding the selected category into groups, then expanding the selected group into individual events within that group. Any changes done to the event apply to just that event within the selected group.

To set the Event Attributes by event level:

1. In the Log > Settings page, click the arrow on the left to expand the category that contains the group with the event you want to edit.
2. Click the arrow on the left to expand the group that contains the event you want to edit.
3. Click the Edit icon in the right-most column of the row with the event you want to edit. The Edit Log Event dialog for that event is displayed.

# Edit Event 'Send Log to FTP'

Event Priorityinform

Enable

Frequency Filter Interval

Display Events in Log Monitor

☒

60

seconds

Send Events as Email Alerts

☐

Multiple Values

seconds

Report Events via Syslog

☐

Multiple Values

seconds

Use This Syslog Server Profile

?

Report Events via IPFIX

☐

Multiple Values

seconds

Include Events in Log Digest

☒

Report Events via SNMP Trap

☐

Multiple Values

seconds

SNMP OID Name(Trap Type)

23

Send Alerts to E-mail Address

Leave color settings unchanged

☐

☒ = current color (click button to change)

Cancel

Save

4. Follow the steps in [Configuring Event Attributes Globally](#).

## About Filename Logging

The Security Services > Application Control group provides the Filename Logging event. Application Control Filename Logging allows the administrator to be notified of each filename or URIs of interest that Application Control has explicitly identified as it processes packets or flows.

CATEGORY	COLOR	ID	PRIORITY	GUI	ALERT	SYSLOG	TRAP	IPFIX	EMAIL	EVENT COUNT
▼ Security Services			debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1664
▶ Anti-Spyware			debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Anti-Virus			debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▼ Application Control			debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Application Control Detection Alert		1154	debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Application Control Prevention Alert		1155	debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Filename Logging		1574	debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
▶ Attacks			debug	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0

The notification uses the Log mechanism where the output can be shown in several message formats, such as on the Monitor > Logs > System Logs page or by Syslog. For Syslog, the message-id for an Application Control Filename Log is 1574 and it has a message template of Filename: %s, where the value substituted for %s can be a filename or URI identified by Application Control.

Filename Logging events can occur when the following requirements are met:

- Enable App Control – Application Control is enabled per zone from the Object > Match Objects > Zones page and globally on the Policy > Rules and Policies > App Control.
- Enable Filename Logging – Filename Logging is enabled on the Log > Settings page.
- Logging is enabled for the App Control Filename Logging event id=1574 – Enable GUI or Syslog with appropriate filtering on the Log > Settings page.

Filename Logging works with the following protocols:

- HTTP
- FTP
- NetBios/CIFS
- SMTP
- POP3
- IMAP

Gateway Anti-Virus does not need to be enabled.

With HTTP, if the server response does not have a filename in its headers, the last portion of the URL that the client requested is used.

If the entire filename cannot be captured because of any reason, (for example, the filename was too long or it straddles multiple packets or any other reason), the prefix portion that was captured is logged and an asterisk is appended to it in the log entry.

## Syslog

Syslog and NetFlow are two different technologies that serve different purposes. Syslog is a logging protocol used to collect and store log messages from devices on a network, while NetFlow is a network protocol used to collect and analyze network traffic data.

When it comes to the usage of both technology, whether to use Syslog or NetFlow depends on the specific needs and requirements. Both technologies can be useful for different purposes, and it may be beneficial to use both in combination to gain a comprehensive view of network activity.

Here are some potential benefits of using Syslog over NetFlow:

### Benefits of Syslog over NetFlow

Syslog	NetFlow
Syslog is widely supported by a variety of devices and systems, making it a flexible and universal logging solution.	NetFlow provides more detailed and granular information about network traffic, including source and destination IP addresses, port numbers, and protocol types. This can be useful for identifying patterns and trends in network usage, and for troubleshooting performance issues.
Syslog can be configured to send log messages to a central server, allowing for easy storage and centralized management of log data.	NetFlow data can be analyzed in real-time, allowing network administrators to quickly identify and respond to potential issues as they arise.
Syslog can be used to collect and store log messages from a variety of sources, including servers, routers, switches, and other network devices.	NetFlow is more efficient than Syslog, as it uses a standardized and compressed format for data transmission. This can be beneficial in environments with high volumes of network traffic, as it can reduce the load on network devices and servers.

In addition to displaying event messages in the GUI, the SonicWall security appliance can send the same messages to an external, user-configured Syslog Server for viewing. The Syslog message format can be selected in Syslog Settings and the destination Syslog Servers can be specified in the Syslog Servers table.

SonicWall Syslog captures all log activity and includes every connection source and destination name and/or IP address, IP service, and number of bytes transferred. SonicWall Syslog support requires an external server running a Syslog daemon; the UDP Protocol is configurable.

SonicWall has fully compatible Syslog viewers, such as GMS / Analyzer that can generate useful reports based on received Syslog messages. When GMS or Analyzer has been enabled, the destination hosts are automatically added as one of the Syslog Servers. Other Syslog Servers can be added as needed. For more information about adding Syslog Servers, see About Event Profiles.



**NOTE:** SonicWall Syslog support requires an external server running a Syslog daemon on a UDP Protocol. The default is UDP, but you can choose a different protocol.

Packet data can be sent to Syslog Servers. For information on how to configure this option, contact SonicWall Support.

### About Event Profiles

By configuring events globally for all Syslog Servers, the events generated from all the modules in the system are reported to all the configured Syslog Servers. This generates huge amounts of Syslog traffic that might cause issues, such as reduced performance and packet loss. Syslog Server profiling, known as Event Profiling, allows more granular control by configuring events by Syslog server instead of globally. Also, there can be multiple groups of Syslog servers, with different events reported to different groups of servers. You can specify up to 24 Event Profiles, with up to 7 Syslog Servers configured for each Event Profile, for a maximum of 168 Syslog Servers per firewall.



**IMPORTANT:** A GMS server used for Syslog must belong to the Profile 0 group. Only Profile 0 group, therefore, can have up to 8 servers total (7 Syslog Servers and 1 GMS server).


The Event Profile is used, along with the Server Name and Port, to uniquely identify a Syslog Server in the Syslog Server table. This allows multiple rows to have same Name, Port combination with different Profiles.

Therefore, a Syslog Server can be a member of more than one Event Profile group.

### About Syslog Server Profiling

This feature provides the ability to configure the settings for each Syslog server independently, instead of using the global settings for all the servers. In previous releases, the events generated from all the modules in the system were reported to all the configured Syslog servers. Depending on the deployment, this generates a huge amount of Syslog traffic and can cause performance issues or even packet loss.

With Syslog Server Profiling, the following new functionality is available:


 NOTE: Recommended maximum of 10 Syslog Servers users would use the dedicated syslog profiles allocated (exception for model NSsp 15700 Series).

- Syslog messages can be sent using different settings for different Syslog servers
- There can be multiple groups of Syslog servers
- Different events can be configured to be reported to different groups of Syslog servers

All the settings in the Log > Syslog page except Enable NDPP Enforcement for Syslog Server can be configured independently for each row in the Syslog Servers table. This allows Syslog messages to be rendered with different settings for different servers, and each server can have its own Rate Limiting options.

Enable/Disable sending of Syslog messages to a specific Syslog server. The settings for Enhanced Syslog and ArcSight format can also be configured individually.

All these settings can be configured from the SonicOS web interface and from the command line interface (CLI.) For convenience, the global settings can be used to configure all servers.

 NOTE: The Override Syslog Settings with Reporting Software Settings option has been removed. As the Syslog servers have their own independent settings, this option is no longer needed.

### Using a GMS/Analytics Server for Syslog

GMS/Analytics can be enabled or disabled only on the Device > Log > Settings page (for enabling and configuring GMS/Analytics, see SonicOS 7.1 System Administration Guide).

When using a GMS/Analytics server for Syslog, the following restrictions apply:

- The Event Profile must be 0.
- The Syslog Facility must be Local Use 0.
- The Syslog Format must be Default.
- The Syslog ID must be firewall.

When firewall is managed using GMS/Analytics, only the global settings can be configured from GMS/Analytics. So, if a global setting is changed, it affects all the servers. The settings for an individual server cannot be configured, as GMS/Analytics does not support those tags. When adding a new Syslog Server, therefore, only the hostname and port can be configured; all other fields contain default values.

When GMS/Analytics is enabled, the GMS/Analytics server is added to the Event Profile 0 group in the Syslog Servers table. It cannot be added to any other Profile groups. The events in the GMS/Analytics group in the Device > Log > Settings page have Profile 0 and cannot be changed. Other events can have a different Profile.

## Syslog Settings

The Device > Log > Syslog page enables you to configure the various settings you want when you send the log to a Syslog server. You can choose the Syslog facility and the Syslog format.

NOTE: If you are using SonicWall's Global Management System (GMS) to manage your firewall, the Syslog Format is set to Default and the Syslog ID is set to firewall. Therefore, these fields are grayed-out and cannot be modified. All other fields, however, can still be customized as needed.

To configure Syslog settings on your firewall:

1. Navigate to Device > Log > Syslog page.



2CB8ED69468C / Device / Log / Syslog

Syslog Settings

Syslog Servers

Enhanced Syslog Fields Settings

Configure

ArcSight CEF Fields Settings

Configure

Enable NDPP Enforcement for Syslog Server

☐

Display Syslog Timestamp in UTC

☐

Cancel

Accept

2. During adding a Syslog sever, If you selected Enhanced Syslog as Syslog Formats, under the Enhanced Syslog Fields Settings, click the Configure icon. The Enhanced Syslog Fields Settings pop-up dialog displays.
3. Select the Enhanced Syslog options to log. By default, all options are selected; the Host and Event ID options are dimmed as they cannot be changed. To:
  - Select all options, click Enable All.
  - Deselect all options, click Disable All.
  - Select only some options, either:
    - Click Disable All, then select only those options to log.
    - Deselect only those options to not log.
4. Click Save.
5. During adding a Syslog sever, If you selected ArcSight as Syslog Formats, under the ARCSight CEF Fields Settings, click the Configure icon. ArcSight CEF Fields Settings pop-up dialog displays.
6. Select the ArcSight options to log. By default, all options are selected; the Host and Event ID options are dimmed as they cannot be changed. To:
  - Select all options, click Enable All.
  - Deselect all options, click Disable All.
  - Select only some options, either:
    - Click Disable All, then select only those options to log.
    - Deselect only those options to not log.
7. Click Save.
8. Select the Enable NDPP Enforcement for Syslog Server.
9. Select the Display Syslog Timestamp in UTC.
10. Click Accept.

## About SonicOS

2CB8ED6942A4 / Device / Log / Syslog

Configuration ☒ Non-Config

Syslog Settings

Syslog Servers

+ Add
Enable All
Disable All
Delete All
Refresh

<input type="checkbox"/>	#	EVENT PROFILE	SERVER NAME	SERVER PORT	SERVER TYPE	SYSLOG FACILITY	SYSLOG FORMAT	SERVER ID	ENABLE
<input type="checkbox"/>	1	0	10.5.92.108 (Test)	514	syslog-server	local-use0	default	firewall	<input type="checkbox"/>

Total: 1 item(s)

#	Serial Number.
Event Profile	Profile configured for the Syslog Server.
Server Name	IP address and name of the Syslog Server.
Server Port	Port of the Syslog Server.
Server Type	Type of the Server.
Syslog Facility	Server Facility of the Syslog Server; for a list of Server Facilities, see Syslog Facility.
Syslog Format	Format expected by the Syslog Server: <ul style="list-style-type: none"> <li>• Default (default)</li> <li>• WebTrends</li> <li>• Enhanced Syslog</li> <li>• ArcSight</li> </ul>
Server ID	ID configured for the Syslog Server; default is firewall.
Enable	Indicates whether the Syslog Server is enabled and allows you to enable or disable the sending of Syslog messages to a specific Syslog Server.
Configure	Contains the Edit and Delete icons for a Syslog Server. As a GMS server cannot be deleted or configured through the Device > Log > Syslog page, these two icons are dimmed.

### Adding a Syslog Server

To add a Syslog server to the firewall.

1. Go to Device > Log > Syslog page.
2. Click Syslog Servers tab.
3. Click Add. The Add Syslog Server dialog appears.


4. Specify the Event Profile for this server in the Event Profile field. The minimum value is 0 (1 group), the maximum is 23 (24 groups), and the default is 0. Each group can have a maximum of 7 Syslog servers.



NOTE: For GMS, the Event Profile must be 0.

5. Select the Syslog server name or IP address from the Name or IP Address drop-down menu. Messages from the firewall are then sent to the servers.
6. If your Syslog server does not use default port 514, type the port number in the Port field.
7. Select the Server Type from the drop-down options. select Syslog Server or Analyzer.
8. From the Syslog Format drop-down menu, select the Syslog format:

#### **SYSLOG FORMATS**

Default	Default SonicWall Syslog format.  NOTE: For GMS, the Syslog format must be Default.
WebTrends	WebTrends Syslog format. You must have WebTrends software installed on your system.
Enhanced Syslog	Enhanced SonicWall Syslog format.
ArcSight	ArcSight Syslog format. The Syslog server must be configured with the ArcSight Logger application to decode the ArcSight messages.


9. The Syslog Facility might be left as the factory default. Optionally, however, from the Syslog Facility drop-down menu, select the Syslog Facility appropriate to your network:

 NOTE: For GMS, the Syslog format must be Local Use 0.

#### **SYSLOG FACILITY**

Kernel	UUCP Subsystem	Local Use 0
User-Level Messages	Clock Daemon (BSP Linux)	Local Use 1
Mail System	AUTHPRV Security/Authorization Messages	Local Use 2
System Daemons	FTP Daemon	Local Use 3
Security/Authorization Messages	NTP Subsystem	Local Use 4
Messages Generated Internally by syslogd	Log Audit	Local Use 5
Line Printer Subsystem	Log Alert	Local Use 6
Network News Subsystem	Clock Daemon (Solaris)	Local Use 7

10. In the Syslog ID field, enter the Syslog ID. The default is firewall.  
A Syslog ID field is included in all generated Syslog messages, prefixed by id=. Therefore, for the default value, firewall, all Syslog messages include id=firewall. The ID can be set to a string consisting of 0 to 32 alphanumeric and underscore characters.
11. Optionally, to limit events logged and therefore, prevent the internal or external logging mechanism from being overwhelmed by log events, select Enable Event Rate Limiting.

 NOTE: Event rate limiting is applied regardless of Log Priority of individual events.

Specify the maximum number of events in the Maximum Events Per Second field; the minimum number is 0, the maximum is 1000, and the default is 1000 per second.

12. Optionally, to limit events logged and therefore, prevent the internal or external logging mechanism from being overwhelmed by log events, select Enable Data Rate Limiting.



NOTE: Data rate limiting is applied regardless of Log Priority of individual events.

Specify the maximum number of bytes in the Maximum Bytes Per Second field; the minimum is number is 0, the maximum is 1000000000, and the default is 10000000 bytes per second. This control limits data logged to prevent the internal or external logging mechanism from being overwhelmed by log events.

13. To Bind To VPN Tunnel and Create Network Monitor Policy in NDPP mode:
  - a. Optionally, choose an interface from the Local Interface drop-down menu.
  - b. Optionally, choose an Interface from the Outbound Interface drop-down menu.
14. Click Add.

## Editing a Syslog Server

To edit a Syslog Server:

1. Hover over on the Syslog Server which you want to edit and click the Edit icon. The Edit Syslog Server dialog displays.

**Edit Syslog Server**

Event Profile

Name or IP Address

Port

Server Type

Syslog Format

Syslog Facility

Syslog ID

Enable Event Rate Limiting ☐

Maximum Events Per Second

Enable Data Rate Limiting ☐

Maximum Bytes Per Second

**BIND TO VPN TUNNEL AND CREATE NETWORK MONITOR POLICY IN NDPP MODE**

Local Interface

Outbound Interface

2. Follow the appropriate Step 4 through in Adding a Syslog Server.

## Enabling Syslog Servers



IMPORTANT: You can enable a GMS Syslog Server only on the Device > Settings > Administration page; see SonicOS 7.1 System Administration Guide.


To enable a single Syslog Server:

1. Select the toggle button in the Enable column.

To enable all Syslog Servers:

1. Select the Syslog servers and click Enable All.

### Disabling Syslog Server


 **IMPORTANT:** You can disable a GMS Syslog Server only on the Device > Settings > Administration page; see SonicOS 7.1 System Administration Guide.  
To disable a single Syslog Server:

1. Deselect the toggle button in the Enable column.

To disable all Syslog Servers:

1. Select the Syslog servers and click Disable All.

### Deleting Syslog Servers

 **IMPORTANT:** You can delete a GMS Syslog Server only on the Device > Settings > Administration page; see SonicOS 7.1 System Administration Guide.

To delete a single Syslog Server:

1. Mouse over on the Syslog server which you want to delete and select the Delete icon.

To delete all Syslog Servers:

1. Select the Syslog servers and click Delete All.

### Automation

The Device > Log > Automation page includes settings for configuring the SonicWall to send log files using Email and configuring mail server settings.

2CB8ED6942A4 / Device / Log / Automation

Email Settings | Mail Server Settings | FTP log Automation

### EMAIL LOG AUTOMATION

Send Log to Email Address:

Send Alerts to Email Address:

Send User Creation and Enablement Notification to Email Address:

Include All Log Information: ☐

Send Log:

Every:

At (24-Hour Format):

Email Format:

---

### EMAIL AUDIT RECORDS AUTOMATION

Send Audit Records to Email Address:

Send Audit Records:

Every:

At (24-Hour Format):

Email Format:

---

### HEALTH CHECK EMAIL NOTIFICATION

Email Schedule:

Send to Email Address:

Email Subject:

Email Body:

## Email Settings

This section describes the procedure for automating email dispatching. You can also send an email of logs manually at any time.

Email Settings | Mail Server Settings | FTP log Automation

### EMAIL LOG AUTOMATION

Send Log to Email Address:

Send Alerts to Email Address:

Send User Creation and Enablement Notification to Email Address:

Include All Log Information: ☐

Send Log:

Every:

At (24-Hour Format):

Email Format:

- Send Log to Email address – To receive the Log Digest through email, enter your email address ([username@mydomain.com](mailto:username@mydomain.com)). After being sent, the Log Digest is cleared from the SonicWall memory. If this field is left blank, the Log Digest is not emailed.
- Send Alerts to Email address – To be emailed immediately when attacks or system errors occur, enter your email address ([username@mydomain.com](mailto:username@mydomain.com)) as a standard email address or an email paging service. If this field is left blank, email alert messages are not sent.
- Send User Creation and Enablement Notification to Email Address – To be emailed immediately when a user has been created and enabled, enter your email address ([username@mydomain.com](mailto:username@mydomain.com)). If this field is left blank, email notifications are not sent.
- Send Log – Determines the frequency of sending Log Digest files. The options in the drop-down menu are:
  - When Full – This setting is the default.
  - Weekly – Select the day of the week the Log Digest is sent in Every drop-down menu and enter the time of day in 24-hour format in the At (24-Hour Format) field.
  - Daily – Enter the time of day the Log Digest is to be sent in 24-hour format in the At (24-Hour Format) field.
- Email Format – Select whether log emails are sent in Plain Text or HTML format or as a CSV Attachment from the drop-down menu.

- Include All Log Information – Select to have all information included in the log report. If not selected, only readable column data is sent.
- To view the logs, click Show Log Monitor at the bottom.
- If finished configuring settings on this page, click Accept.

## Email Audit Records Automation

Use this feature to send audit records to specific e-mail addresses automatically on a predefined schedule.

The screenshot shows the 'EMAIL AUDIT RECORDS AUTOMATION' configuration form. It includes the following fields and options:

- Send Audit Records to Email Address:** A text input field containing 'example@example.com'.
- Send Audit Records:** A dropdown menu set to 'When Full'.
- Every:** A dropdown menu set to 'Sunday'.
- At (24-Hour Format):** A text input field with a calendar icon on the right.
- Email Format:** A dropdown menu set to 'Plain Text'.

To send audit records to specific email addresses:

1. In the Send to Email Address field, enter the email address(es) of the recipient(s) to notify.
2. In Send Audit Records, define when:
  - Daily – Enter the time of day in 24-hour format in the At (24-Hour Format) field.
  - Weekly – Select the day of the week in Every drop-down menu and enter the time of day in 24hour format in the At field.
  - When Full – This setting is the default.
3. Select Email Format:
  - Plain Text
  - HTML
  - CSV Attachment
4. To view the logs, click Show Log Monitor.
5. When all the fields are configured, click Accept.

## Health Check Email Notification

The Health Check Email Notification section enables you to create a predefined email notification with a set subject and body at the times specified by the selected schedule.

The screenshot shows the 'HEALTH CHECK EMAIL NOTIFICATION' configuration form. It includes the following fields and options:

- Email Schedule:** A dropdown menu set to 'Disabled'.
- Send to Email Address:** A text input field.
- Email Subject:** A text input field containing '[2CB8ED6942A4]'.
- Email Body:** A large text area for composing the email body.
- Buttons:** 'Show Log Monitor' (disabled), 'Cancel' (disabled), and 'Accept' (active).

**To set up a Health Check Email Notification:**

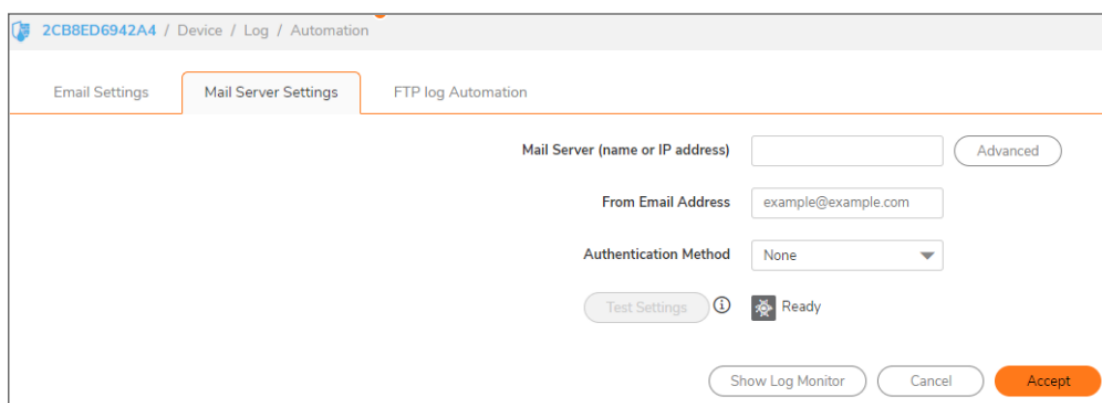
1. From the Email Schedule drop-down menu, select a predefined schedule, Create new schedule, or Disabled.
2. In the Send to Email Address field, enter the email address of the recipient(s) to notify.
3. In the E-mail Subject field, enter the subject of the email. The Firewall Name is included by default. The

Firewall Name is configured on Policy > Firewall, and is the appliance serial number by default.

4. In the Email Body field, enter the body of email.
5. To view the logs, click Show Log Monitor at the bottom..
6. If finished configuring settings on this page, click Accept.

## Mail Server Settings

The mail server settings allow you to specify the name or IP address of your mail server, the from Email address, and authentication method. You can also enter a POP3 server name or IP address, with username and password.

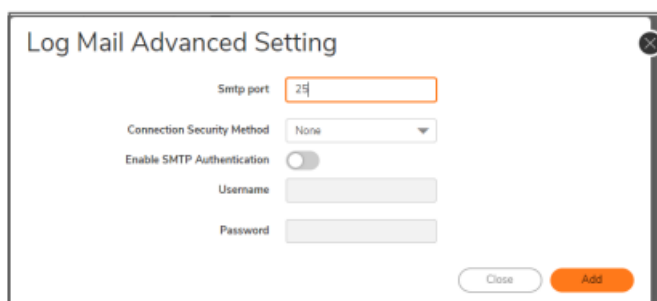


- Mail Server (name or IP address) – Enter the IP address or FQDN of the email server used to send your log emails in this field.



NOTE: If the Mail Server (name or IP address) is left blank, log and alert messages are not emailed.

- Advanced – The Advanced button displays the Log Mail Advanced Setting dialog.



- Smtp port – Enter the SMTP port used for email. The default port number is 25.
- Connection Security Method – Select a security method for the email from the drop-down menu:
  - None (default)
  - SSL/TLS
  - STARTTLS
- Enable SMTP Authentication – Select to enable SMTP authentication for the emails, then enter the following. This option is disabled by default.
- Username
- Password
- From Email Address – Enter the Email address you want to display in the From field of the message.
- Authentication Method – You can use the default None or select POP Before SMTP.
- POP3 Server (name or IP address) – Enter the IP address or FQDN of the email server used to send your log emails in this field.



- Username – Enter the POP3 username.
  - Password – Enter the password for the POP3 account.
  - If finished configuring settings on this page, click Accept.
- Clicking on Show Log Monitor displays you all the system logs.

## FTP Log Automation

FTP log automation enables the administrator to send logs to an FTP server. It is similar to Email Log Automation in the following aspects:

- You can select text, HTML, or CSV file format
- You can select detailed or concise log information
- You can select a predefined time schedule. In addition to the defined schedule, logs are sent when the administrator clicks Restart and when the log is full.

2CB8ED6942A4 / Device / Log / Automation

Email Settings Mail Server Settings **FTP log Automation**

Send Log to FTP ☐

FTP Server 0.0.0.0

Username admin

Password

Directory logs

Send Log When Full

Every Sunday

At (24-Hour Format)

File Format Plain Text

Include All Log Information ☐

Show Log Monitor Cancel Accept

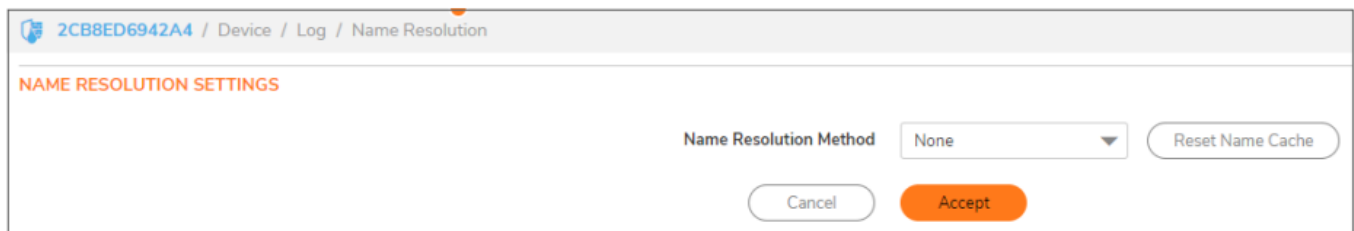
### To configure FTP log automation settings:

1. Navigate to the Device > Log > Automation page and select FTP Log Automation tab.
2. Select Send Log to FTP to enable FTP log automation. If this option is not selected, all the other options are grayed out.
3. For FTP Server, enter the IPv4 address of the FTP server.
4. For Username, enter the username for authenticating to the FTP server.
5. For Password, enter the password for the FTP server account.
6. For Directory, enter the destination directory on the FTP server. The default is logs.
7. From the Send Log drop-down menu, select the frequency for sending the logs to the FTP server. Choose Daily, Weekly, or When Full. The default is When Full.

8. Select the day of the week for sending the logs from the drop-down menu next to Every field. This is used for a Weekly schedule.
9. Select the hour and minute of the day in 24 hour format in the two fields next to the At (24-Hour Format).  
The time is used for Daily and Weekly schedules.
10. From the File Format drop-down menu, select one of Plain Text, HTML, or CSV Attachment as the format in which the logs are sent.
11. Select Include All Log Information to have all information included in the log report. If not selected, only readable column data is sent.
12. If finished configuring settings on this page, click Accept.  
Clicking on Show Log Monitor displays you all the system logs.

## Name Resolution

The Device > Log > Name Resolution page includes settings for configuring the name servers used to resolve IP addresses and server names in the log reports.



The SonicWall network security appliance uses a DNS server or NetBIOS to resolve all IP addresses in log reports into server names. It stores the names/address pairs in a cache, to assist with future lookups. You can clear the cache by clicking Reset Name Cache button.

### Selecting Name Resolution Settings

The firewall appliance can use DNS, NetBIOS, or both to resolve IP addresses and server names. In the Name Resolution Method list, select:

- None: The security appliance does not attempt to resolve IP addresses and Names in the log reports.
- DNS: The security appliance uses the DNS server you specify to resolve addresses and names.
- NetBIOS: The security appliance uses NetBIOS to resolve addresses and names. If you select NetBIOS, no further configuration is necessary.
- DNS then NetBIOS: The security appliance first uses the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it tries again with NetBIOS.

### Specifying the DNS Server

You can choose to specify DNS servers, or to use the same servers as the WAN zone.

1. Select Specify DNS Servers Manually or Inherit DNS Settings Dynamically from WAN Zone. The second choice is selected by default.
2. If you selected to specify a DNS server, enter the IP address for at least one DNS server on your network. You can enter up to three servers.
3. Click Accept.

## Reports

The firewall can complete a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. Generate these reports from the Device > Log > Reports page.

**NOTE:** SonicWall Analyzer provides a comprehensive Web-based reporting solution for firewalls. For more information on SonicWall Analyzer, go to <http://www.SonicWall.com>.

## Data Collection

The Device > Log > Reports page includes these functions:

- Data Collection – Enable Start Data Collection to begin log analysis. When log analysis is enabled, the button label changes to Stop Data Collection.
- Click Reset icon to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the firewall is restarted.
- Click Refresh icon to update the real-time data in the table.

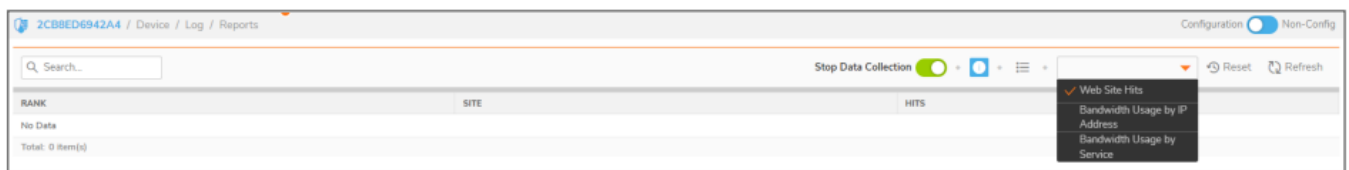
### View Data

Select the desired report from Report View:

- Web Site Hits (default)
- Bandwidth Usage by IP Address

- Bandwidth Usage by Service

The length of time analyzed by the report is displayed in the Current Sample Period.



### Web Site Hits

Selecting Web Site Hits from the drop-down displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The Web Site Hits report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites. For information on blocking inappropriate Web sites refer to the Objects > Profile Objects > Content Filter command in SonicOS 7.1 Objects Guide.

### Bandwidth Usage by IP Address

Selecting Bandwidth Usage by IP Address from the drop-down displays a table showing the IP address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.

### Bandwidth Usage by Service

Selecting Bandwidth Usage by Service from the drop-down displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, and so on, and the number of megabytes received from the service during the current sample period.

The Bandwidth Usage by Service report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.

### Backup Logs Information

The logging information can be retained in an on-board database. It can also preserve the data in the event of a loss of power. These features apply if the appliance has had additional non-volatile storage built into the it and the appliance is running SonicOS 6.5.1 or later.

The maximum number of entries that can be stored on the log database is increased to 50,000 for all platforms, but the amount of space available is driven by the size of the built-in storage module and space allocated for logging.

If storage is available, backups of the logs are taken automatically and requires no configuration. They can also be manually deleted.



**NOTE:** Loading the Log Reports page can be slower when there are too many entries in the log database. Similarly, exporting a log report can be slower.

To delete backups:

1. Navigate to the Device > Settings > Storage > Files page.
2. Under Logs group, click Purge. The backups are deleted.

## AWS

The Device > Log > AWS Logs page allows configuration of the Amazon Web Services (AWS) endpoint to which the logs are sent along with settings affecting the frequency with which the data is posted.

2CB8ED69468C / Device / Log / AWS

### CLOUDWATCH LOGS

Enable Logging

☐

Region

North Virginia

Log Group Name

Log Stream Name

Synchronization Interval

60

secs.

Force Sync

Send Log when full

☒

### LOG STATUS

Overall Status

Logging Disabled

Latest Push Status

Started request to push logs

Push Requests

0

Log Messages Sent

0

Bytes Sent

0

Connections Failed

0

Test Configuration

Reset Count

Accept

Logged events generated on the firewall can be sent to the AWS CloudWatch Logs service. From there, the data can be used by AWS hosted analysis tools such as ElasticSearch and Kibana.

## Enabling AWS Logs

**NOTE:** In order to send the logs from SonicOS to Amazon CloudWatch Logs, you must first create a Log Group and a Log Stream in AWS. If you already have an Identity Access Management (IAM) user account with the appropriate permissions to access CloudWatch Logs from the AWS Console:

1. Navigate to the CloudWatch section.
2. Select the Logs item in the left navigation menu. Ensure that you have selected the appropriate AWS Region for the logs to be stored. As with many AWS services, CloudWatch Logs is region-specific.
3. Create the Log Group.
4. Create the Log Stream.

To enable AWS logs in SonicOS:

1. Navigate to the Device > Log > AWS page.
2. In the CloudWatch Logs section, select Enable Logging.
3. Select the Region in which you created a Log Group and Log Stream in the AWS Console. (You can change the region used by the firewall either on this page or on the Network > System > AWS Configuration page.)
4. Enter the names of the Log Group and Log Stream that you created in the AWS Console that holds the logs sent to AWS CloudWatch Logs.
5. The logs are sent at the specified Synchronization Interval. Change the value of the interval (in seconds) to suit your needs.
6. Optionally, you can click Force Sync to manually synchronize with your AWS Console settings.

7. Click Accept.

## SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services at <https://sonicwall.com/pes>.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

## About This Document

SonicOS Device Log Administration Guide

Updated – December 2023

Software Version – 7.1

232-005865-00 Rev A

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products.

EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

## Open Source Code


SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to: General Public License Source Code Request

Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035

## SonicOS 7.1 Device Log Administration Guide SonicWall Support

---

### Documents / Resources

	<p><a href="#">SONICWALL SonicOS 7.1 Device Log</a> [pdf] User Guide SonicOS 7.1 Device Log, SonicOS 7.1, Device Log, Log</p>
---	---

### References

- [SonicWall.com](#)
- [sonicwall.com/](#)
- [SonicWall Community | Technology and Support](#)
- [MySonicWall](#)
- [sonicwall.com/pes](#)
- [MySonicWall](#)
- [sonicwall.com/legal](#)
- [sonicwall.com/legal/end-user-product-agreements/](#)
- [sonicwall.com/support](#)
- [sonicwall.com/support/contact-support](#)
- [sonicwall.com/support/technical-documentation/](#)
- [sonicwall.com/support/technical-documentation/?language=English&category=Firewalls&resources=Administration%20Guide&version=7.1](#)
- [sonicwall.com/support/technical-documentation/?language=English&category=Firewalls&resources=Getting%20Started%20Guide](#)
- [sonicwall.com/support/technical-documentation/?q=sonicos%20api&language=English](#)
- [sonicwall.com/support/technical-documentation/sonicos-7-1-api](#)
- [sonicwall.com/support/technical-documentation/sonicos-7-1-monitor](#)
- [sonicwall.com/support/technical-documentation/sonicos-7-1-system](#)
- [User Manual](#)