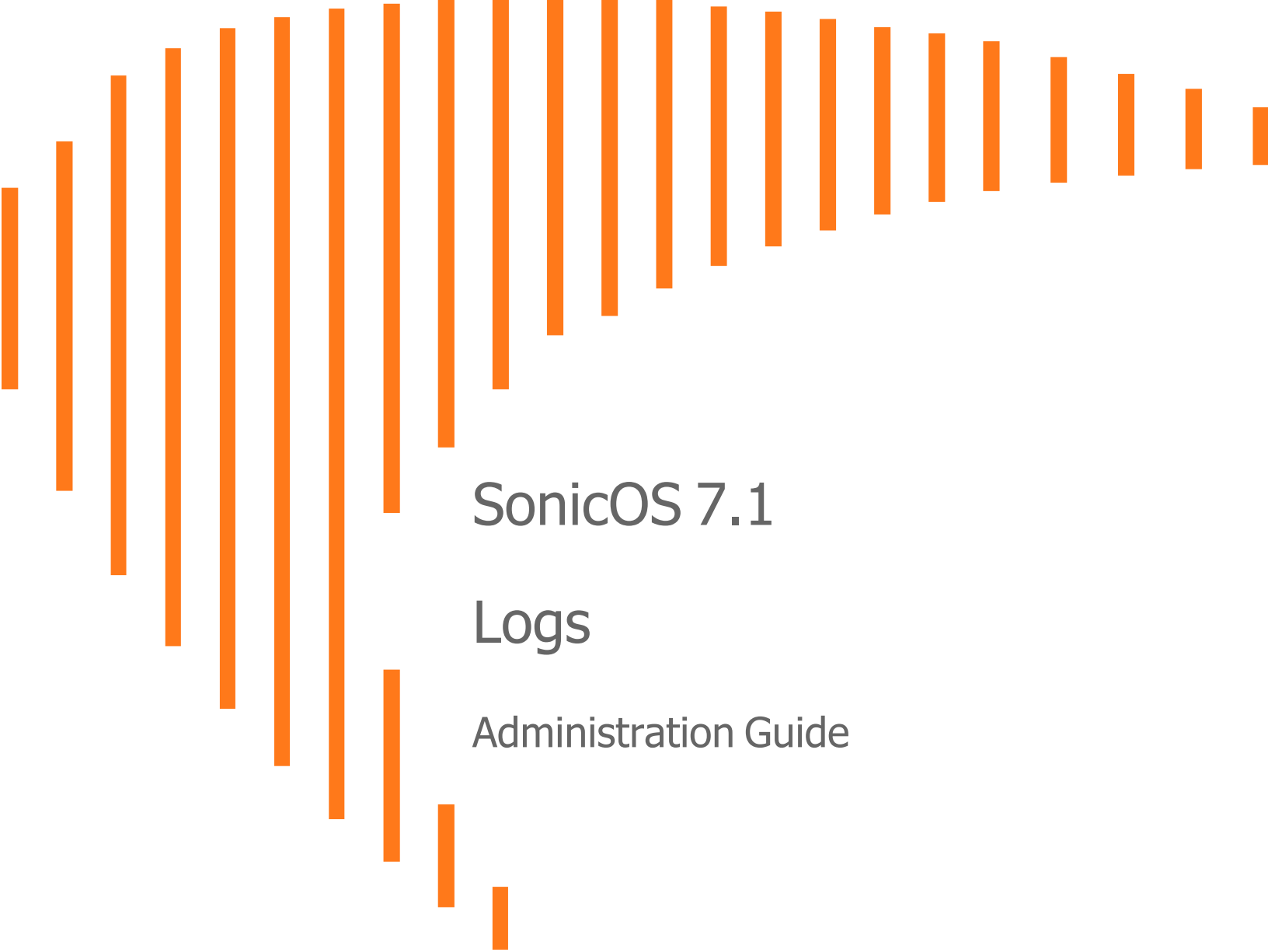




SonicOS 7.1

Logs

Administration Guide

SONICWALL[®]

Contents

About SonicOS	3
Working with SonicOS	3
SonicOS Workflow	5
How to Use the SonicOS Administration Guides	6
Guide Conventions	7
System Logs	8
Viewing System Logs	8
System Log Functions	8
Display Options	10
Filtering the View	13
Auditing Logs	14
What is Configuration Auditing	14
Benefits of Configuration Auditing	14
What Information is Recorded	15
What Information is Not Recorded	15
Audit Recording in High Availability Configurations	15
Modifying and Supplementing Configuration Auditing	16
SNMP Trap Control	16
E-CLI Commands	16
Auditing Record Storage and Persistence	16
Managing the Audit Logs Table	17
Viewing Auditing Logs	17
Manually Emailing Auditing Logs	18
Exporting Auditing Logs	18
Refreshing the Auditing Logs	18
Displaying the Auditing Logs on the console	18
Auditing All Parameters During Addition	19
Threat Logs	20
Viewing Threat Logs	20
Threat Log Functions	20
Display Options	21
SonicWall Support	24
About This Document	25

About SonicOS

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.

Topics:

- [Working with SonicOS](#)
- [SonicOS Workflow](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

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:

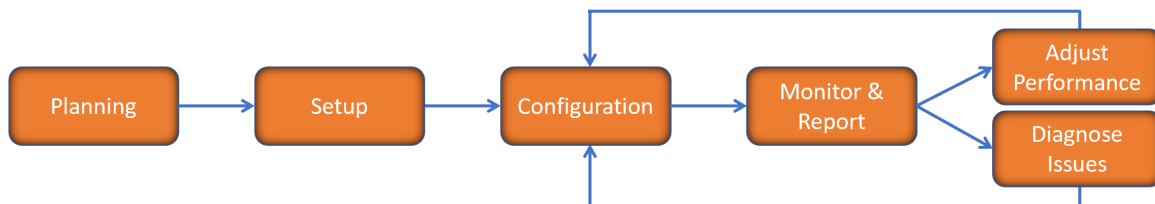
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPS bandwidth issues; built-in SD-WAN, 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:

- [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.

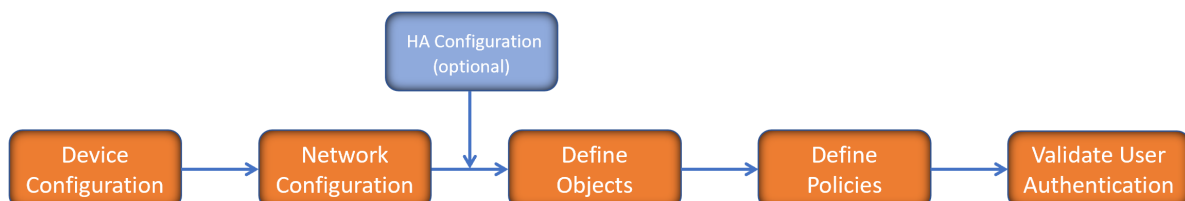


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). 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.

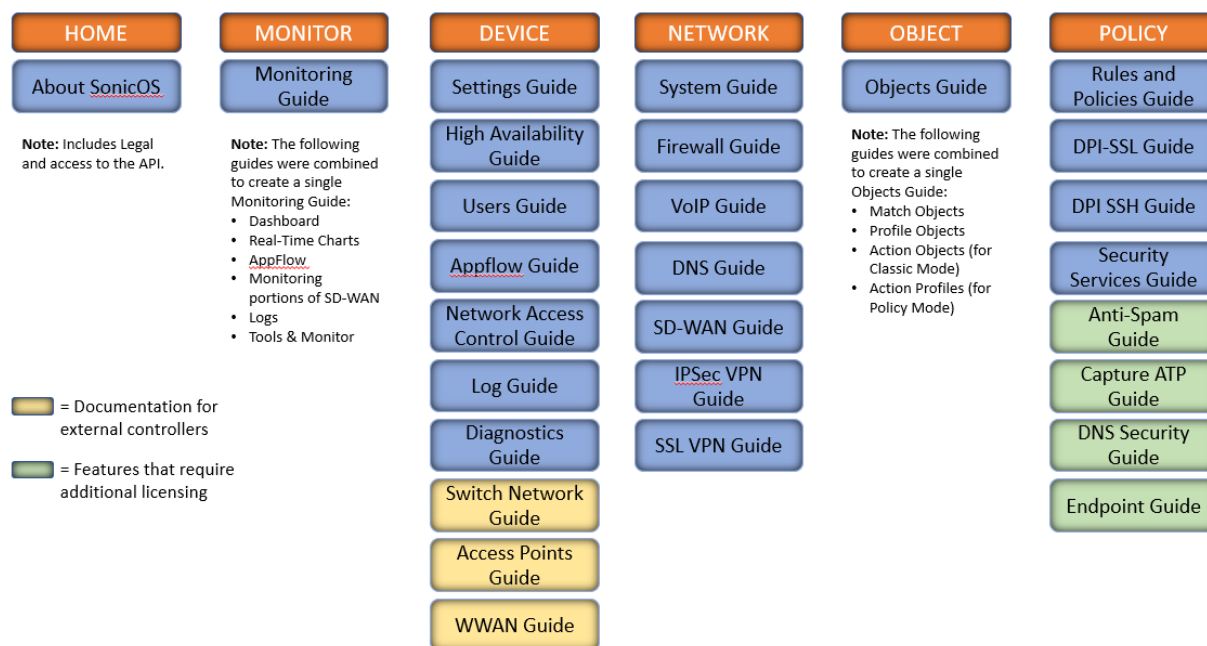


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement 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:

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **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.

System Logs

The SonicWall network security appliance maintains an Event log for tracking potential security threats.

Topics:

- [Viewing System Logs](#)
- [System Log Functions](#)
- [Display Options](#)
- [Filtering the View](#)

Viewing System Logs

To view system events, navigate to **MONITOR | Logs > System Logs** page.

For a description of the:

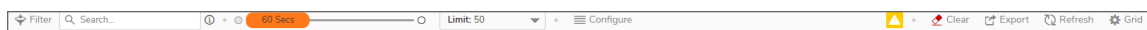
- Functions, see [System Log Functions](#)
- Columns, see [Display Options](#)

System Log Functions

The System Log table provides numerous settings to allow you to navigate, view, and export results. Table columns can be customized, so that you can view full data on any event, or only the data you need. Table entries can be sorted to display in either ascending or descending order.

To sort the entries in the Event Log, click the column heading. The entries are sorted by ascending or descending order. The arrow to the right of the column name indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the Event Log contains various functions. Functions pertaining only to Event Logs are described in the below table.



SYSTEM EVENT LOG FUNCTIONS

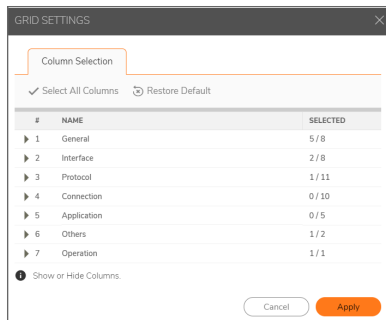
Option	Function	Action
 Filter	Filter	Set the filter for any specific log in the Event Log. You can set the filters based on GENERAL, SOURCE, and DESTINATION categories. For more information, refer to Filtering the View .
 Search...	Search	The Event Log displays the log entries that match the search string.
 Refresh	Refresh	Click to refresh the system log data.
 Configure	Configure Log	Click this link and you are navigated to DEVICE Log > Settings to configure the items which needs to be tracked in the Event Log.
 Clear	Clear Logs	Click to clear the logs from the table.
 Export	Export	Click to export the logs in CSV, TXT files, and email

Display Options

Customize the Events log to display as many or few columns that meet your needs.

To select which columns to display:

1. Navigate to **MONITOR | Logs > System Logs**.
2. Click  **Grid** icon . The **Grid Settings** dialog displays:



3. Select the items you want to appear as columns in the System Log.

General	
General information about the log event.	
Time	Local date and time the event occurred. i IMPORTANT: This option is selected by default. It is dimmed, and cannot be deselected.
ID	Identifying number for the event. i IMPORTANT: This option is selected by default. It is dimmed, and cannot be deselected.
Category	Category of the event. This option is selected by default.
Group	Group designation of the event.
Event	Name of the event.
Msg Type	Type of message; usually Standard Message String.
Priority	Priority level of the event, such as Inform (information) or Error. i IMPORTANT: This option is selected by default.
Message	Information about the event.

Interface	Information about the protocol of the packet triggering the event.	
	Source	Name of the source device, if applicable. This option is selected by default.
	Source IP	IP address of the source device.
	Source Port	Port number of the source.
	Source Interface	Source network and IP address, if applicable.
	Destination	Name of the destination device, if applicable. This option is selected by default.
	Destination IP	IP address of the destination device.
	Destination Port	Port number of the destination.
	Destination Interface	Destination network and IP address, if applicable.
Protocol	Information about the NAT policy in effect, if any.	
	Source Name	Protocol source name.
	Source NAT IP	Source address from the Source NAT IP address pool.
	Source NAT Port	Port number for the Source NAT.
	In SPI	Indicates whether the ingress packet is in Stateful Packet Inspection (SPI) mode, if applicable.
	Destination Name	Protocol destination name.
	Destination NAT IP	Destination address from the Source NAT IP address pool.
	Destination NAT Port	Port number for the Destination NAT.
	Out SPI	Indicates whether the egress packet is in Stateful Packet Inspection (SPI) mode, if applicable.
	IP Protocol	Protocol used to send error and control messages, if known. This option is selected by default.
	ICMP Type	ICMP packet's ICMP type, if known.
	ICMP Code	ICMP packet's ICMP code, if known.

Connection	Information about SPI, Access and IDP Rules, and policies, if any.	
	TX Bytes	Number of bytes transmitted.
	RX Bytes	Number of bytes received.
	Access Rule	Name of the Access Rule triggering the event, if any.
	NAT Policy	Name of the NAT policy.
	VPN Policy	Name of the VPN policy triggering the event, if any.
	User Name	Name of the user whose action triggered the event.
	Session Time	Duration of the session before the event.
	Session Type	Type of session triggering the event.
	IDP Rule	Name of the IDP Rule triggering the event, if any.
	IDP Priority	Priority of the IDP Rule.
Application	Information about the application being used.	
	HTTP OP	NPCS object op requestMethod HTTP OP code.
	URL	URL of the NPCS object op requestMethod HTTP OP code.
	HTTP Result	HTTP result code (such as, 200, 403) of Website hit rpkt cn1Label Packet received.
	Block Category	Block category that triggered the event.
	Application	The application being used.
Others	Information about the user, session, and application, if known.	
	FW Action	Configured firewall action. If no action has been specified, displays N/A.
	Notes	Includes notes. This option is selected by default.
Operation	Action	Provides option to disable the events.

- When done, click **Apply** to preserve any changes or click **Restore Default** to revert back to the default settings.

You can perform the following actions on the System Logs page:

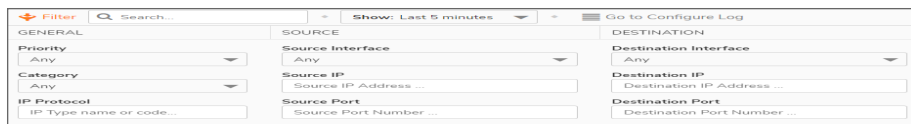
- To export the logs in CSV, TXT files, and email, click **Export** icon and select the required format
- To clear the logs from the table, click **Clear Logs** icon
- To refresh the page, click **Refresh** icon
- To view more details of the log, click the triangle icon of the log

Filtering the View

The Filter View input field at the top left corner of the System Log enables you to narrow your search using drop-down options and search strings.

To filter the System Event logs:

1. Navigate to **MONITOR | Logs > System Logs**.
2. Click **Filter** icon.



The screenshot shows the 'Filter' view interface. At the top, there is a search bar with a magnifying glass icon and the text 'Search...'. To the right of the search bar is a dropdown menu labeled 'Show: Last 5 minutes' and a button labeled 'Go to Configure Log'. Below these are three main filter sections: 'GENERAL', 'SOURCE', and 'DESTINATION'. Each section contains several filterable fields with dropdown menus and text input boxes.

GENERAL	SOURCE	DESTINATION
Priority Any	Source Interface Any	Destination Interface Any
Category Any	Source IP Source IP Address ...	Destination IP Destination IP Address ...
IP Protocol IP Type name or code...	Source Port Source Port Number ...	Destination Port Destination Port Number ...

3. Select any filtering scheme you want. Filter on just one field or you can filter on all of them. In the General, Source and Destination fields, you can enter a partial string to filter on.
4. Click **Accept**.
OR
Click **Reset** to clear the filters applied.

Auditing Logs

This section describes in detail the recording feature that collects and records information on any changes in the security appliance configuration. To access this feature, navigate to **MONITOR | Logs > Auditing Logs** in the SonicOS web management interface.

What is Configuration Auditing

Configuration auditing is a feature that automatically records any configuration changes that an administrator attempts from one of the available user interfaces, web management (via HTTP and HTTPS), command line (via console or SSH), or SonicWall GMS. A configuration auditing records table is created to record all attempted configuration changes, both successful and failed. With configuration auditing, SonicOS archives the history of its configuration changes, so that the administrator or others can later revisit and analyze the records. This feature is enabled by default for the platforms where it is available.

Benefits of Configuration Auditing

Auditing of configuration change records can be useful as described below:

- Automatic documentation of any configuration changes performed by an administrator
- Assistance in troubleshooting unexpected changes in run-time system behavior
- Visibility, continuity, and consistency where there are several administrators, either simultaneously or consecutively. Each administrator has access to a record of changes performed or attempted by all other administrators.
- Third party integration with Firewall Manager, SEIM systems, logging and reporting solutions
- Compliance with regulations such as SOX, FISMA, NIST, DISA STIP

What Information is Recorded

Configuration auditing generates a record for every configuration change. The record includes:

- Which parameter was changed
- When the change was made
- Who made the change
- From where the change was made
- Details of the change, such as the previous and subsequent values

What Information is Not Recorded

The following are not included in the Configuration Auditing operation:

- Importing a Settings File - Configuration changes due to importing a settings file are currently not recorded by the configuration auditing feature. Since all current settings are cleared prior to applying imported configurations, the assumption is that all existing configurations are modified.
- WXA configuration settings — SonicOS does not audit any configuration changes in WAN Acceleration. Some settings are saved on the WXA instead of the firewall, although the settings can be configured from the SonicOS web management interface.
- ZEBOS settings for BGP/OSPF/RIP routing configurations — SonicOS stores these settings as one long string of ZEBOS CLI commands. Records of changes made by these commands are not duplicated in the configuration auditing operation.
- Anti-Spam Junk Store applications — Configuration settings changed through a proxy server running a junk store are excluded from configuration auditing.
- Licensing - All aspects of system licensing are authenticated through MySonicWall, and are not recorded through configuration auditing.
- Uploading a file from **Home > Capture ATP** does not audit uploading a file from the page, because the contents of this page do not reside on the firewall.

Audit Recording in High Availability Configurations

The Configuration Auditing operation records changes individually for each device. It does not synchronize the recorded information between appliances in an HA pair. When the active HA unit next synchronizes with the standby HA unit, it sends configuration changes to the standby unit. The synchronization operation information

updates the auditing record of the standby device in the pair. On the standby unit, the auditing record indicates that the configuration changes it recorded came from the active unit.

Modifying and Supplementing Configuration Auditing

Configuration Auditing operations can be modified and supplemented through the following:

SNMP Trap Control

SNMP (Simple Network Management Protocol) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks. SNMP traps allow the user to monitor security appliance status and configuration through a Management Information Database (MIB). Configuration auditing works in conjunction with SNMP by giving the user the option to enable a trap for each logged event collected during a network configuration change, whether successful or failed.

E-CLI Commands

E-CLI (Enterprise Command Line Interface) commands are available for configuration auditing record setting and display, for those administrators who like to work from the command line. You can use the following E-CLI commands to enable or disable configuration auditing and to view records:

to work with settings:

```
config(C0EAE49CE84C)# log audit settings
```

```
(config-audit)# enable
```

```
(config-audit)# debug
```

```
(config-audit)# auditall
```

```
(config-audit)# commit
```

to show audit records:

```
(config-audit)# show log audit view
```

Auditing Record Storage and Persistence

Configuration auditing records are saved to non-volatile storage (such as flash), so that records can be restored, if required, after a reboot. The number of records saved is directly proportional to the capability of the device, as

defined in the product matrix below. Higher-end platforms can store more records than lower-end devices. Devices with no flash or smaller flash capacity do not support configuration auditing.

All configuration auditing records, on any platform, are deleted when the appliance is rebooted with factory defaults.

Managing the Audit Logs Table

The administrator can manage the auditing records in many useful ways. The following activities are available:

Topics:

- [Viewing Auditing Logs](#)
- [Manually Emailing Auditing Logs](#)
- [Exporting Auditing Logs](#)
- [Refreshing the Auditing Logs](#)
- [Displaying the Auditing Logs on the console](#)
- [Auditing All Parameters During Addition](#)

Viewing Auditing Logs

The **MONITOR | Logs > Auditing Logs** page displays all the configuration auditing records. It allows a user to view, search, and sort the records.

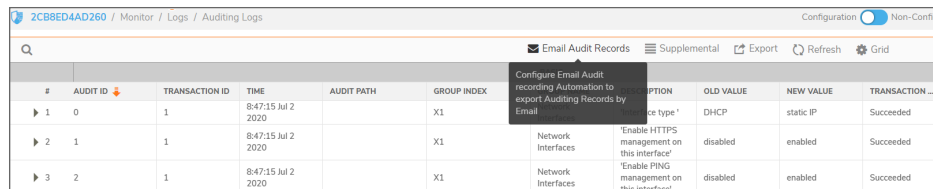
- The first column is expandable to display the summary of the log entry.
- There are also buttons for **Select all Columns** and **Restore Default** for ease of operation. Click **Grid Settings** icon to perform the desired action.
- The user can search for a specific string pattern and highlight the matched results, if any are found.
- Failed configuration changes are marked in red.
- All columns are sortable.

2CB8ED4AD260 / Monitor / Logs / Auditing Logs										
Configuration ☒ Non-Config										
Email Audit Records Supplemental Export Refresh Grid										
#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	GROUP NAME	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION ...
▶ 1	0	1	8/47/15 Jul 2 2020		X1	Network Interfaces	'Interface type '	DHCP	static IP	Succeeded
▶ 2	1	1	8/47/15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8/47/15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded
▶ 4	3	1	8/47/15 Jul 2 2020		X1	Network Interfaces	'Static IP Address'	0.0.0.0	10.5.193.110	Succeeded
▶ 5	4	1	8/47/15 Jul 2 2020		X1	Network Interfaces	'Static Subnet Mask'	255.255.255.0	255.255.254.0	Succeeded
▶ 6	5	1	8/47/15 Jul 2 2020		X1	Network Interfaces	'Static Gateway IP Address'	0.0.0.0	10.5.192.1	Succeeded

Manually Emailing Auditing Logs

When a valid mail server and email address are configured, the user can click the email button on the tool bar of the Auditing Records page to manually email auditing records at any time. The button is disabled if either the mail server or the email address is not configured under **DEVICE | Log > Automation**.

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

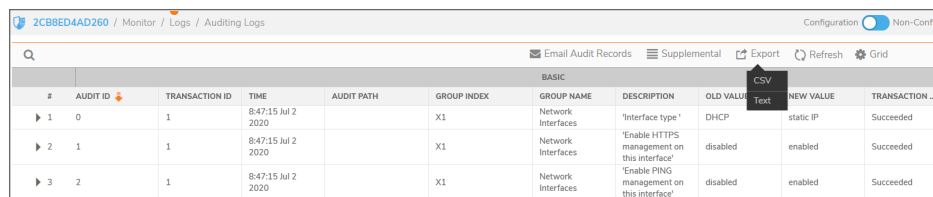


The screenshot shows the 'Auditing Logs' page with a toolbar containing 'Email Audit Records', 'Supplemental', 'Export', 'Refresh', and 'Grid'. A tooltip for 'Email Audit Records' is visible, stating: 'Configure Email Audit recording Automation to export Auditing Records by Email'.

#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	OPTION	OLD VALUE	NEW VALUE	TRANSACTION ...
1	0	1	8:47:15 Jul 2 2020						
2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	Succeeded
3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	Succeeded

Exporting Auditing Logs

There are two export options for auditing records. You can export the records as a text file or as a CSV file.

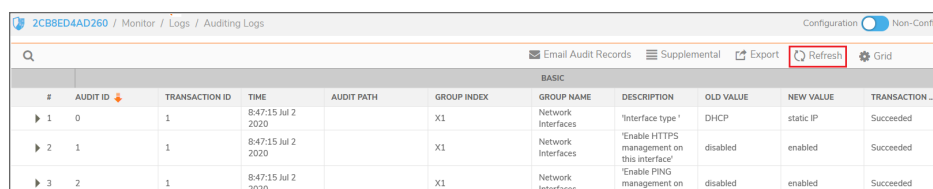


The screenshot shows the 'Auditing Logs' page with the 'Export' button highlighted. A dropdown menu is open, showing 'CSV' and 'Text' options.

#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	GROUP NAME	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION ...
1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded

Refreshing the Auditing Logs

The **Refresh** button provides a way to refresh the page and display the latest auditing records, as seen below:



The screenshot shows the 'Auditing Logs' page with the 'Refresh' button highlighted in the toolbar.

#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	GROUP NAME	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION ...
1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded

Displaying the Auditing Logs on the console

Click **Supplemental > Display Auditing Records on Console** option to display the auditing records on the console in a text format.

2CB8ED4AD260 / Monitor / Logs / Auditing Logs

Configuration ☒ Non-Config

Q

Email Audit Records Supplemental Export Refresh Grid

BA

Display Auditing Records on Console

GR

Audit Supplemental Parameter Changes

#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	BA	GR	ALUE	NEW VALUE	TRANSACTION ...
▶ 1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
▶ 2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded

Auditing All Parameters During Addition

By default, configuration auditing only logs significant changes, defined as changes where the new value of the parameter is different from the default value. Click **Supplemental > Audit Supplemental Parameter Changes** option to record all parameter changes during an addition activity, even when the new values are the same as the default values.

2CB8ED4AD260 / Monitor / Logs / Auditing Logs

Configuration ☒ Non-Config

Q

Email Audit Records Supplemental Export Refresh Grid

BA Display Auditing Records on Console

GR Audit Supplemental Parameter Changes

ALUE

#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	BA	GR	ALUE	NEW VALUE	TRANSACTION ...
▶ 1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type'	DHCP	static IP	Succeeded
▶ 2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled	enabled	Succeeded
▶ 3	2	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable PING management on this interface'	disabled	enabled	Succeeded

Threat Logs

This section describes in detail the recording feature that collects and records information on any changes in the security appliance configuration. To access this feature, navigate to **MONITOR | Logs > Threat Logs** in the SonicOS web management interface.

Q Search...

①

*

○

2 Mins

○

○

Custom

Limit: 50

▼

⚠

*

📄 Export

🔄 Refresh

⚙ Grid

#	TIMESTAMP	USERNAME	THREAT				TIME		IP ADDRESS	
#	TIME	USER NAME	VIRUS	INTRUSION	SPYWARE	BOTNET	START TIME	LAST UPDATED	INITIATOR IP	RESPONDER
No Data										

Topics:

- [Viewing Threat Logs](#)
- [Threat Log Functions](#)
- [Display Options](#)

Viewing Threat Logs

To view threat events, navigate to **MONITOR | Logs > Threat Logs** page.

For a description of the:

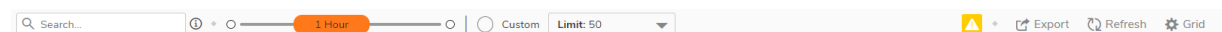
- Functions, see [Threat Log Functions](#)
- Columns, see [Display Options](#)

Threat Log Functions

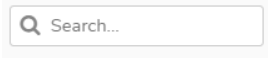
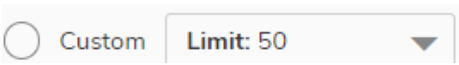
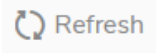
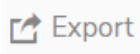
The Threat Log table provides numerous settings to allow you to navigate, view, and export results. Table columns can be customized, so that you can view full data on any event, or only the data you need. Table entries can be sorted to display in either ascending or descending order.

To sort the entries in the Event Log, click the column heading. The entries are sorted by ascending or descending order. The arrow to the right of the column name indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

The top row of the Event Log contains various functions. Functions pertaining only to Event Logs are described in the below table.



SYSTEM EVENT LOG FUNCTIONS

Option	Function	Action
	Search	The Event Log displays the log entries that match the search string.
	Time Interval	Set the slider to filter the Event Log based on the time interval for the Event Log. You can set the slider anywhere between 60 Sec to 365 days.
	Custom	Select the interval for the Event Log. The event logs displays the maximum entries in the table based on selection. • 10 • 25 • 50 • 100 • 250 • 500 • 1000 • 8000 (Max)
	Refresh	Click to refresh the log data.
	Export	Click to export the logs.

Display Options

Customize the Events log to display as many or few columns that meet your needs.

To select which columns to display:

1. Navigate to **MONITOR | Logs > Threat Logs**.
2. Click  **Grid** icon . The **Grid Settings** dialog displays:

GRID SETTINGS

Column Selection

✓ Select All Columns

↺ Restore Default

#	NAME	SELECTED
▶ 1	Timestamp	1 / 1
▶ 2	Application	2 / 2
▶ 3	URL	3 / 3
▶ 4	UserName	1 / 1
▶ 5	Threat	4 / 4
▶ 6	Time	2 / 2
▶ 7	IP Address	2 / 2
▶ 8	IP	1 / 1
▶ 9	Port	2 / 2
▶ 10	Country	2 / 2
▶ 11	FileName	1 / 1
▶ 12	Capture ATP	1 / 1
▶ 13	Interface	2 / 2
▶ 14	BWM	2 / 2
▶ 15	Statistics	4 / 4
▶ 16	Status	2 / 2
▶ 17	Policies	7 / 7
▶ 18	MAC	2 / 2
▶ 19	Miscellaneous	5 / 5

ⓘ Show or Hide Columns.

Cancel

Apply

3. Select the items you want to appear as columns in the Threat Log.

Category Name	Column
Timestamp	Time
Application	Application
	Component
URL	URL
	URL Rating
	URL Severity
User Name	User Name
Threat	Virus
	Intrusion
	Spyware
	Botnet
Time	Start Time
	Last Updated

Category Name	Column
IP Address	Initiator IP
	Responder IP
IP	Protocol Name
Port	Initiator Port
	Responder Port
Country	Initiator
	Responder
FileName	FileName
Capture ATP	Action
Interface	Initiator Interface
	Initiator Interface
BWM	Inbound Priority
	Outbound Priority
Statistics	All Counters
	Initiator Bytes
	Responder Bytes
Status	Flow Status
	Blocked Reason
Policies	Security Rule
	NAT Rule
	Init Route Rule
	Resp Route Rule
	Decryption SSL Rule
	Decryption SSH Rule
	DoS Rule
MAC	Init MAC
	Responder MAC
Miscellaneous	Initiator Gateway
	Responder Gateway
	Initiator VPN Name
	Gateway VPN Name

- When done, click **Apply** to preserve any changes or click **Restore Default** to revert back to the default settings.

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 Logs Administration Guide
Updated - December 2023
Software Version - 7.1
232-006095-00 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