SonicOS 7.0

Logs

Administration Guide

SONICWALL®

Contents

1

System Logs

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

Topics:

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

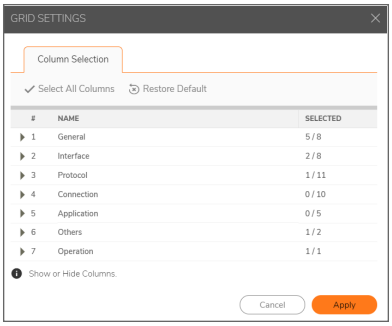
Option	Function	Action
Filter	Filter	Set the filter for any specific log in the Event Log. You can set the filters based on GENERAL, SOURCE, and DESTINATION categories. For more information, refer to Filtering the View.
Search...	Search	The Event Log displays the log entries that match the search string.
60 Secs	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.
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 Settings** 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. **IMPORTANT:** This option is selected by default. It is dimmed, and cannot be deselected.
	ID	Identifying number for the event. **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. **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.

4. 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:

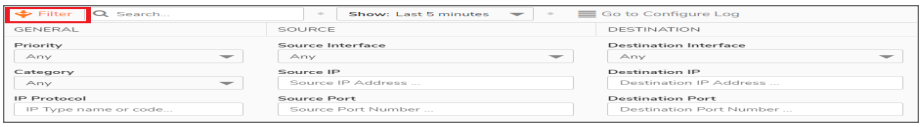
- To export the logs in CSV, TXT files, and email, click **Export** icon and select the required format
- To clear the logs from the table, click **Clear Logs** icon
- To refresh the page, click **Refresh** icon
- To view more details of the log, click the triangle icon of the log

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.



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.

2

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:

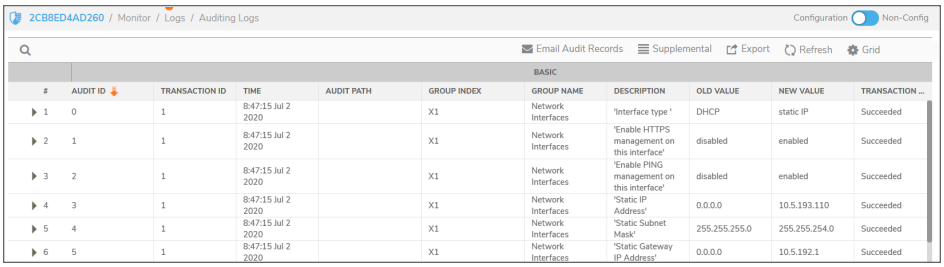
Topics:

- 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.

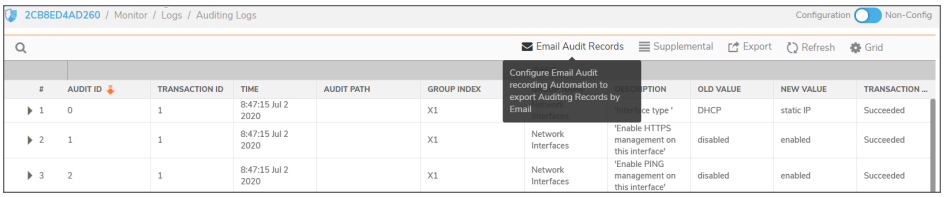


#	AUDIT ID	TRANSACTION ID	TIME	AUDIT PATH	GROUP INDEX	GROUP NAME	DESCRIPTION	OLD VALUE	NEW VALUE	TRANSACTION ...
1	0	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Interface type '	DHCP	static IP	Succeeded
2	1	1	8:47:15 Jul 2 2020		X1	Network Interfaces	'Enable HTTPS management on this interface'	disabled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

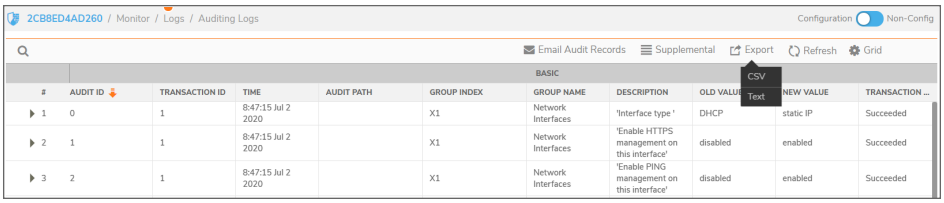
When a valid mail server and email address are configured, the user can click the email button on the tool bar of the Auditing Records page to manually email auditing records at any time. The button is disabled if either the mail server or the email address is not configured under **DEVICE | Log > Automation**.

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



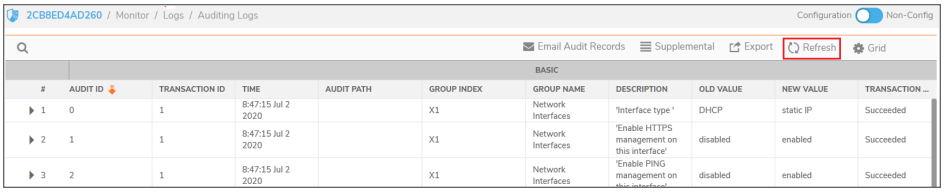
Exporting Auditing Logs

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



Refreshing the Auditing Logs

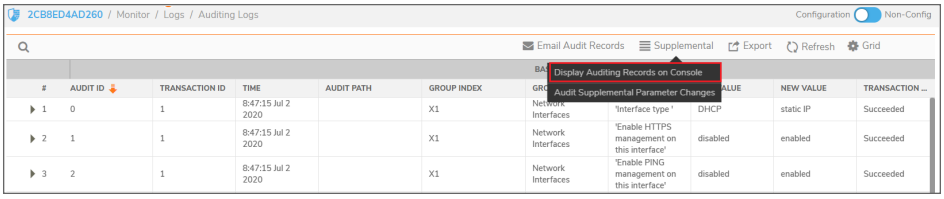
The **Refresh** button provides a way to refresh the page and display the latest auditing records, as seen below:



Displaying the Auditing Logs on the console

To view the auditing records:

1. Navigate to **MONITOR | Logs > Auditing Logs**.
2. Click **Supplemental > Display Auditing Records on Console** option to display the auditing records on the console in a text format.

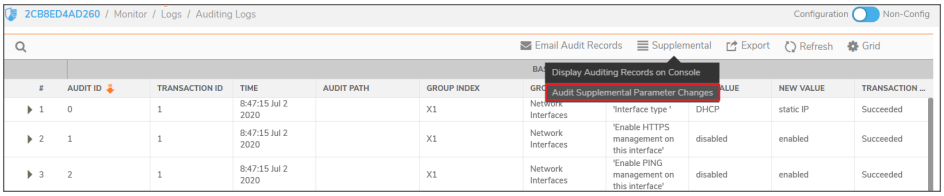


Auditing All Parameters During Addition

By default, configuration auditing only logs significant changes, defined as changes where the new value of the parameter is different from the default value.

To view the updated parameter changes during addition activity:

1. Navigate to **MONITOR | Logs > Auditing Logs**.
2. 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.



3

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.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

SonicOS LogsAdministration Guide
Updated - April 2024
Software Version - 7.0
232-005339-00 Rev C

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