

# SonicWall<sup>®</sup> Management Services System Log

Administration

SONICWALL<sup>®</sup>

# Contents

<b>Configuring Log Settings</b> .....	<b>3</b>
Global Syslog Settings .....	4
Syslog Settings .....	6
Export Log/Alerts .....	7
Syslog Servers .....	8
Adding a Syslog Server .....	9
Editing a Syslog Server .....	10
Enabling Syslog Servers .....	11
Disabling Syslog Servers .....	11
Deleting Syslog Servers .....	11
About Event Profiles .....	11
Health Check E-mail Notification .....	12
Solera Capture Stack .....	13
<b>Configuring Log Categories</b> .....	<b>15</b>
Email Column .....	17
<b>Configuring Name Resolution</b> .....	<b>20</b>
<b>SonicWall Support</b> .....	<b>21</b>
About This Document .....	22

# Configuring Log Settings

## To configure log settings:

- 1 In the left pane, select the global icon, a group, or a SonicWall appliance.
- 2 In the center pane, navigate to **Log > Settings**.
- 3 Start with the top subpage section, **General**.

## Settings

Home / Tenant - LocalDomain / TZ 500 W Running Config ▼

### MAIL SERVER SETTINGS

Mail Server (name or IP Address)	<input type="text"/>	Advanced
From E-mail Address	<input type="text"/>	
Authentication Method	None ▼	
POP Server (name or IP address)	<input type="text"/>	
Username	<input type="text"/>	
Password	<input type="password"/>	<a href="#">?</a>
Firewall Name	<input type="text"/>	

- 4 Enter the IP address or name of the mail server in the **Mail Server (name or IP Address)** field.  
Click on Advanced to define the SMTP server.

#### ADVANCED MAIL SETTINGS

SMTP Port	25
Connection Security Method	None ▼
<input type="checkbox"/> Enable SMTP Authentication	
Username	<input type="text"/>
Password	<input type="password"/>

[Update](#) [Cancel](#)

- **SMTP Port** — Defaults to 25.
  - **Connection Security Method**— None, SSL/TLS, or STARTTLS
  - **Username and Password**
- 5 Enter the email address used for the sender in the **From E-mail Address** field.
  - 6 If your email server requires SMTP authentication, select **POP Before SMTP** in the drop-down menu and enter these options:
    - IP Address of the POP server in the **POP Server (name or IP address)** field.
    - User name in the **Username** field.
    - Password in the **Password** field.

- Enter the name of the SonicWall appliance in the **Firewall Name** field. The firewall name appears in the subject of email sent by the SonicWall appliance. By default, the firewall name is the same as the SonicWall appliance serial number.

**NOTE:** The name of the SonicWall appliance cannot be configured at the group or global level.

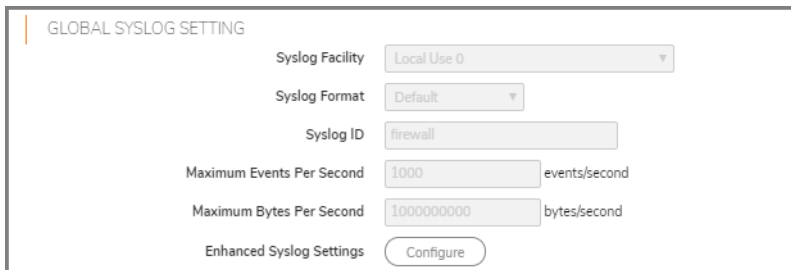
**Topics:**

- [Global Syslog Settings](#)
- [Export Log/Alerts](#)
- [Syslog Servers](#)
- [Solera Capture Stack](#)

# Global Syslog Settings

This section allows 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.

- Navigate to **Log > Settings | Global Syslog Setting**.



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

**Syslog Facility**

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

- From the **Syslog Format** drop-down menu, select the Syslog format:

**Syslog Formats**

- Default** Default SonicWall Syslog format.  
**NOTE:** This format is required for GMS or Reporting software.
- Enhanced Syslog** Enhanced SonicWall Syslog format.

## Syslog Formats

### WebTrends

### ArcSight

- If you selected:
  - Default**, go to [Step 11](#).
  - Enhanced Syslog**, go to [Step 5](#).
- (Optional) If you selected **Enhanced Syslog**, click the **Configure** button. The **Enhanced Syslog Settings** pop-up dialog displays.

The screenshot shows the 'Enhanced Syslog Settings' dialog box. It is organized into several sections, each with a list of options and checkboxes. The sections are:

- GENERAL**: Host (sn), Message (msg), Event ID (m), Category (cat), Group Category (gcat).
- INTERFACE**: Src Interface, Src Mac Addr (srcMac), Dst Interface, Dst Mac Addr (dstMac).
- PROTOCOL**: Src IP (src), Dst IP (dst), Protocol (proto), Src NAT IP (natSrc), Dst NAT IP (natDst), ICMP type (type), Src Port, Dst Port, ICMP code (icmpCode), Src NAT Port, Dst NAT Port.
- CONNECTION**: Bytes Rcvd (rcvd), User (usr), Src VPN Policy (vpnpolicy), Client Policy (rule), Bytes Sent (sent), Conn Duration (cdur), Dst VPN Policy (vpnpolicyDst), Interface stats, Pkts Rcvd (rpkt), Session Type (sess), Src Zone (srcZone), SonicPoint Stats, Pkts Sent (spkt), Session Time (dur), Dst Zone (dstZone).
- APPLICATION**: HTTP OP (op), Application (app), HTTP result (result), GMS Heartbeat, URL (dstname), GMS change URL (Change), Block Reason (code).
- OTHERS**: Counter (n), Anti Spam, NPCS (npcs), App Firewall, Note (note), Raw Data, IDP.

At the bottom of the dialog, there are four buttons: 'Select All', 'Clear All', 'OK', and 'Cancel'.

- (Optional) Select the **Enhanced Syslog** options to log. By default, all options are selected; the **Host (sn)** and **Event ID (m)** options are dimmed as they cannot be changed. To:
  - Select all options, click **Select All**.
  - Deselect all options, click **Clear All**.
  - Select only some options, either:
    - Click **Clear All**, then select only those options to log.
    - Deselect only those options to not log.
- Click **OK**.
- 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=`. So 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.

9 Specify the maximum number of events in the **Maximum Events Per Second** field; the minimum number is 0 per second, the maximum is 1000 per second, and the default is **1000**. This option limits events logged to prevent the internal or external logging mechanism from being overwhelmed by log events.

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

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

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

11 Enter the number of seconds between “heartbeats.” The default value is 60 seconds.

## Syslog Settings

When using a GMS 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.

The screenshot shows a configuration window for Syslog settings. The fields are as follows:

- Event Profile: 0
- Name or IP Address: --Select an address objec
- Port: 514
- Syslog Format: Default
- Syslog Facility: Local Use 0
- Syslog ID: firewall
- Enable Event Rate Limiting:
- Maximum Events Per Second: 1000
- Enable Data Rate Limiting:
- Maximum Bytes Per Second: 10000000
- Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode:
- Local Interface: --Select an interface--
- Outbound Interface: Select a tunnel interface

Buttons: Update, Cancel

1 Specify the maximum number of events in the **Maximum Events Per Second** field; the minimum number is 0 per second, the maximum is 1000 per second, and the default is **1000**. This option limits events logged to prevent the internal or external logging mechanism from being overwhelmed by log events.

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

- Optionally, specify the maximum number of bytes in the **Maximum Bytes Per Second** field; the minimum is 0 bytes per second, the maximum is 100000000 bytes per second, and the default is **10000000**. This control limits data logged to prevent the internal or external logging mechanism from being overwhelmed by log events.

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

Only the global settings can be configured from Management. So, if a global setting is changed, it affects all the servers. The settings for an individual server cannot be configured, as Management 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.

The Management server is added to the Event Profile 0 group in the Syslog Servers table. It cannot be added to any other Profile groups. Therefore, only the Profile 0 group can have 8 servers in total (7 Syslog servers and 1 Management server). All other groups can have only 7 servers. The events in the GMS group in the **Log > Settings** page have Profile 0 and cannot be changed. Other events can have a different Profile.

**NOTE:** Multi bladed platform supports only 2 Syslog servers per profile.

## Export Log/Alerts

EXPORT LOG/ALERTS

EMail Log to

EMail Log Now

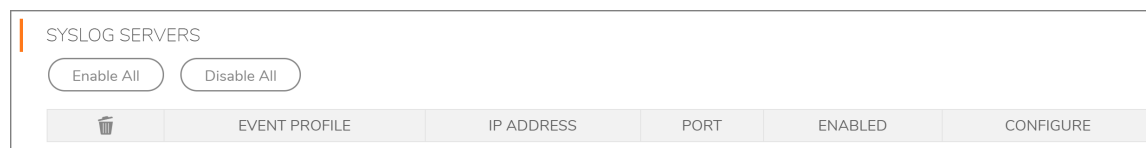
EMail Alerts to

Clear Log Now

Send User Creation and Enablement Notification to E-mail Address

- Email Log to** - To receive the event log via email, enter your email address (*username@mydomain.com*). Once sent, the log is cleared from the SonicWall memory. If this field is left blank, the log is not emailed.
- Email Alerts to** - To be emailed immediately when attacks or system errors occur, enter your email address (*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 E-mail Address** – To be emailed immediately when a user has been created and enabled, enter your email address (*username@mydomain.com*). If this field is left blank, email notifications are not sent.

# Syslog Servers



<b>Event Profile</b>	Profile configured for the Syslog Server.
<b>IP Address</b>	IP address of the Syslog Server.
<b>Port</b>	Port of the Syslog Server.
<b>Enabled</b>	Indicates whether the Syslog Server is enabled and allows you to enable or disable the sending of Syslog messages to a specific Syslog Server.
<b>Configure</b>	Contains the <b>Edit</b> and <b>Delete</b> icons for a Syslog Server. As a GMS server cannot be deleted or configured through the <b>Log &gt; Syslog</b> page, these two icons are dimmed.

Global settings affect all servers. For example, a change in a global format changes the format of all the servers to the selected value.

## Topics:

- [Syslog Servers](#)
- [Editing a Syslog Server](#)
- [Enabling Syslog Servers](#)
- [Disabling Syslog Servers](#)
- [Deleting Syslog Servers](#)



# Adding a Syslog Server

To add a Syslog server to the firewall.

- 1 Navigate to **Log > Settings | Syslog Servers** section.
- 2 Click **Add**. The **Add Syslog Server Address** dialog appears.

The screenshot shows the 'Add Syslog Server Address' dialog box with the following fields and values:

- Event Profile: 0
- Name or IP Address: --Select an address objec
- Port: 514
- Syslog Format: Default
- Syslog Facility: Local Use 0
- Syslog ID: firewall
- Enable Event Rate Limiting:
- Maximum Events Per Second: 1000
- Enable Data Rate Limiting:
- Maximum Bytes Per Second: 10000000
- Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode:
- Local Interface: --Select an interface--
- Outbound Interface: Select a tunnel interface

Buttons: Update, Cancel

- 3 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. .

**(i) NOTE:** For GMS, the Event Profile must be **0**.

**(i) NOTE:** Multi bladed platform supports only 2 Sysylog servers per profile.

- 4 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.
- 5 If your Syslog server does not use default port **514**, type the port number in the **Port Number** field.
- 6 Select the Syslog format from the **Syslog Format** drop-down menu. The default is **Default**; for all the options, see [Syslog Formats](#).

**(i) NOTE:** For GMS, the Syslog format must be **Default**.

- 7 Select the Syslog Facility from the **Syslog Format** drop-down menu. The default is **Local Use 0**; for all the Syslog Facilities, see [Syslog Facility](#).

**(i) NOTE:** For GMS, the Syslog format must be **Local Use 0**.

- 8 Optionally, to limit events logged and thus prevent the internal or external logging mechanism from being overwhelmed by log events, select **Enable Event Rate Limiting**.

**(i)** | **NOTE:** Event rate limiting is applied regardless of Log Priority of individual events.

- a 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. This option .
- 9 Optionally, to limit events logged and thus prevent the internal or external logging mechanism from being overwhelmed by log events, select **Enable Data Rate Limiting** .

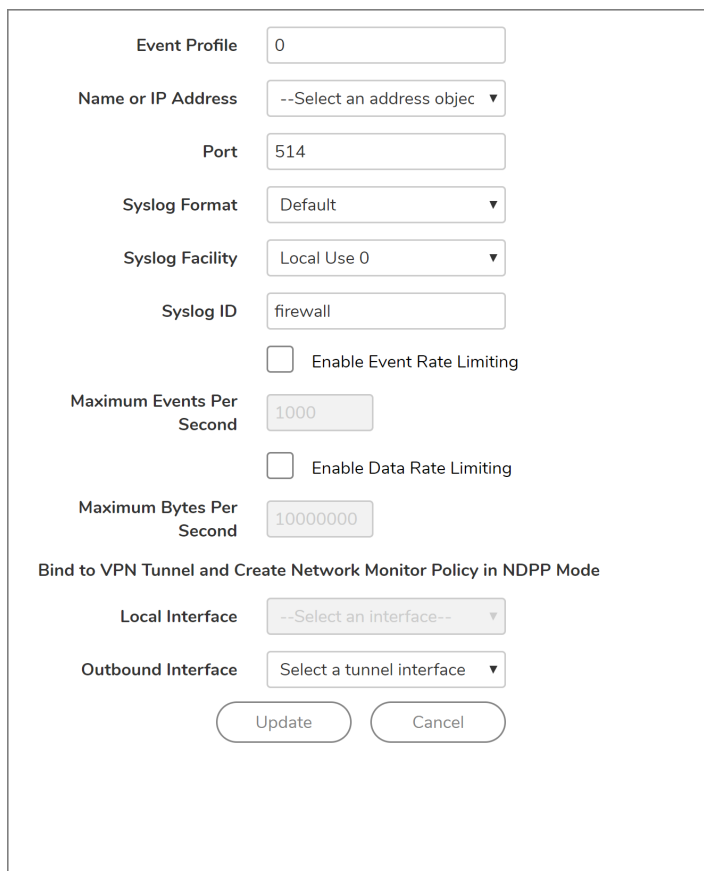
**(i)** | **NOTE:** Data rate limiting is applied regardless of Log Priority of individual events.

- a 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.
- 10 To bind to a VPN tunnel and create a 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.
  - 11 Click **Update**.

# Editing a Syslog Server

## To edit a Syslog Server:

- 1 Click the **Edit** icon in the **Configure** column. The **Edit Syslog Server** dialog displays.



The screenshot shows the 'Edit Syslog Server' dialog box with the following fields and options:

- Event Profile: 0
- Name or IP Address: --Select an address objec
- Port: 514
- Syslog Format: Default
- Syslog Facility: Local Use 0
- Syslog ID: firewall
- Enable Event Rate Limiting
- Maximum Events Per Second: 1000
- Enable Data Rate Limiting
- Maximum Bytes Per Second: 10000000
- Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode
- Local Interface: --Select an interface--
- Outbound Interface: Select a tunnel interface
- Buttons: Update, Cancel

- 2 Follow the appropriate [Step 4](#) through [Step 11](#) in [Adding a Syslog Server](#).

# Enabling Syslog Servers

## To enable a single Syslog Server:

- 1 Select the checkbox in the **Enable** column.

## To enable all Syslog Servers:

- 1 Click **Enable All**.

# Disabling Syslog Servers

## To disable a single Syslog Server:

- 1 Deselect the checkbox in the **Enable** column.

### *To disable all Syslog Servers:*

- 1 Click **Disable All**.

## Deleting Syslog Servers


### *To delete a single Syslog Server:*

- 1 Select the **Delete** icon in the **Configure** column.

### *To delete all Syslog Servers:*


- 2 Click **Disable All**.

## About Event Profiles

 **NOTE:** Event Profiling is supported by all firewalls running SonicOS 6.2.7 and above except the SM 9800.

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, which may 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.

 **NOTE:** Multi bladed platform supports only 2 Syslog servers per profile.

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

## Automation

### AUTOMATION

Send Log

Every

At  :00 hours

When Log Overflows  Overwrite Log  
 Shutdown SonicWall

E-mail Format

Include All Log Information

- **Send Log** - Determines the frequency of sending log files. The options in the drop-down menu are
  - **When Full** (default)
  - **Weekly**—Select the day of the week the log is sent in the **every** drop-down menu and enter the time of day in 24-hour format in the **At** field
  - **Daily**.—Enter the time of day the log is to be sent in 24-hour format in the **At** field.
- Select whether to overwrite logs or shut down the device in case of log overflow.
- **E-mail Format** - Select whether log emails should be sent in **Plain Text** or **HTML** format from the drop-down menu.
- **Include All Log Information** - Select to have all information included in the log report.

## Health Check E-mail Notification

The **HEALTH CHECK E-MAIL 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 a configuration window titled "HEALTH CHECK E-MAIL NOTIFICATION". It contains the following fields:

- E-mail schedule**: A drop-down menu currently set to "Disabled".
- Send to E-mail Address**: A text input field.
- E-mail Subject**: A text input field containing "[COEAE4599168]:" followed by a greyed-out area.
- E-mail Body**: A large, empty text area for entering the email body content.

### To set up a Health Check E-mail Notification:

- 1 From the **E-mail Schedule** drop-down menu, select a pre-defined schedule.
- 2 In the **Send to E-mail 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.
- 4 In the **E-mail Body** field, enter the body of email.

# Solera Capture Stack

Solera Networks makes a series of appliances of varying capacities and speeds designed to capture, archive, and regenerate network traffic. The Solera Networks Network Packet Capture System (NPCS) provides utilities that allow the captured data to be accessed in time sequenced playback, that is, analysis of captured data can be performed on a live network via NPCS while the device is actively capturing and archiving data.

## SOLERA CAPTURE STACK

Enable Solera Capture Stack Integration

Server

Protocol

Port

DeepSee Base URL

PCAP Base URL

Base64-encoded Link Icon

Address to link from E-mail Alerts

### To configure your SonicWall appliance with Solera:

- 1 Select the **Enable Solera Capture Stack Integration** option.
- 2 Configure the following options:
  - **Server** - Select the host for the Solera server.
  - **Protocol** - Select either HTTP or HTTPS.
  - **Port** - Specify the port number for connecting to the Solera server. This value changes according to the value entered under **Protocol**.
  - **DeepSee Base URL** - Defines the format for the base URL for the DeepSee path. In the actual URL, the special tokens are replaced with the actual values.
  - **PCAP Base URL** - Defines the format for the base URL for the PCAP path. In the actual URL, the special tokens are replaced with the actual values.
  - **Base64-encoded Link Icon** - Optionally, in the Base64-encoded Link Icon field, you can specify a Base 64-encoded GIF icon to display instead of the default SonicWall logo.

**i** **NOTE:** Ensure the icon is valid and make the size as small as possible. The recommended size is 400x65.

- **Address to link from E-mail Alerts** - Choose between a default LAN or a default WAN server.

The following tokens can be used in the **DeepSee Base URL** and **PCAP Base URL** fields:

- **\$host** - server name or IP address that has the data
- **\$port** - HTTP/HTTPS port number where the server is listening

- **\$usr** - user name for authentication
- **\$pwd** - password for authentication
- **\$start** - start date and time
- **\$stop** - stop date and time
- **\$ipproto** - IP protocol
- **\$scrip** - source IP address
- **\$dstip** - destination IP address
- **\$srcport** - source port
- **\$dstport** - destination port

# Configuring Log Categories

The **Log > Categories** page allows you to view and edit log categories for many features of a firewall. The **Log > Categories** page displays logging data in a series of columns and allows you to configure the logging entries and to reset event counts. You can filter the entries to limit the data display to only those events of interest. You can import and save logging templates.

## Categories

🏠 / Tenant - LocalDomain / FirmwareView

### CATEGORIES

CATEGORY	ID	PRIORITY	GUI	ALERT	SYSLOG	IPFIX	EMAIL	COLOR	EDIT
System		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Log		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Security Services		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Users		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewall Settings		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
High Availability		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3G/4G, Modem, and Module		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Firewall		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wireless		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VoIP		Mixed	<input type="checkbox"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SSL VPN		Inform	<input type="checkbox"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Anti-Spam		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WAN Acceleration		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SD-WAN		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save as Template

Import from Template

Update

Reset

## Categories Column

The Categories column of the Log Categories table has three levels:

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


Clicking the small black triangle expands or collapses the category or group contents.

## ID Column

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



# Priority Column

 **CAUTION:** Changing the Event Priority may have serious consequences as the Event Priority for all categories will be changed. Modifying the Event Priority will affect the Syslog output for the tag “pri=” as well as how the event will be treated when performing filtering by priority level. Setting the Event Priority to a level that is lower than the Logging Level will cause those events to be filtered out. Also, as Managements Service 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 menu is provided that lists the selectable priorities. For categories and groups, the priorities are listed in the dialog when you click the **Configure** button at the end of the row.

The available priorities are:

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

# GUI Column

The **GUI** column shows check boxes that indicate whether this event is displayed in the Log Monitor. For events, you can show or hide the event by selecting or deselecting the check box in the column. For categories and groups, you must use the configure dialog.

# Alert Column

The **Alert** column shows check boxes that indicate whether an Alert message will be sent for this event, group, or category.

# Syslog Column

The **Syslog** column indicates whether the event, group, or category is sent to a Syslog server. 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 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.

# IPFIX Column

The IP Flow Information Export (**IPFIX**) column indicates whether IPFIX is enabled for log events. System logs can be sent to an external server via 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 shows check boxes that indicate whether the log will be emailed to the configured address. For events, these check boxes are configurable in the column. For categories and groups, **Email** is configured in the **Edit Log Group** or **Edit Log Category** dialogs that appear when you click the **Configure** button at the end of the row.

# Color Column

The **Color** column shows the color with which the event, group, or category is highlighted in the **Log Monitor** table.

# Edit Log Category

Set the log category stream filter and event attributes by category level. Log category stream filtering depends on the filters selected in the GUI column, the Alert column, the Syslog column, and the Email column. Any changes done at the category level affect both group and event levels.

The default value for the log category stream filter is zero.

The log category stream filter has three values, as shown in the following images.

## 1 Disabled

EDIT LOG CATEGORY

Event Category **Anti-Spam**

Event Priority **Mixed** ▼

Enable Redundancy Filter Interval

Display Events in Log Monitor  Multiple Values sec

Send Events as Email Alerts  0 sec

Report Events via Syslog  Multiple Values sec

Use this Syslog Server Profile 0 ▼

Report Events via IPFIX  Multiple Values sec

Include Events in Log Digest

Send Log Digest to Email Address

Send Alerts to Email Address  Leave Unchanged  
Multiple Values

Show Events using Color   Leave Unchanged

## 2 Enabled

EDIT LOG CATEGORY

Event Category **3G/4G, Modem, and Module**

Event Priority **Mixed** ▼

Enable Redundancy Filter Interval

Display Events in Log Monitor  Multiple Values sec

Send Events as Email Alerts  Multiple Values sec

Report Events via Syslog  Multiple Values sec

Use this Syslog Server Profile 0 ▼

Report Events via IPFIX  Multiple Values sec

Include Events in Log Digest

Send Log Digest to Email Address

Send Alerts to Email Address  Leave Unchanged  
Multiple Values

Show Events using Color   Leave Unchanged

### 3 Partially Enabled

EDIT LOG CATEGORY

Event Category SSL VPN

Event Priority Inform

Enable Redundancy Filter Interval

Display Events in Log Monitor  Multiple Values sec

Send Events as Email Alerts  Multiple Values sec

Report Events via Syslog  0 sec

Use this Syslog Server Profile 0

Report Events via IPFIX  Multiple Values sec

Include Events in Log Digest

Send Log Digest to Email Address

Send Alerts to Email Address  Leave Unchanged

Multiple Values

Show Events using Color  Leave Unchanged

Update Cancel

# Configuring Name Resolution

## To configure name resolution:

- 1 In the left pane, select the global icon, a group, or a SonicWall appliance.
- 2 In the center pane, navigate to **Log > Name Resolution**.

## Name Resolution

[Home](#) / [Tenant - LocalDomain](#) / [FirmwareView](#)

### NAME RESOLUTION SETTINGS

Name Resolution Method

DNS SETTINGS

Specify DNS Servers Manually

Log Resolution DNS Server 1

Log Resolution DNS Server 2

Log Resolution DNS Server 3

Inherit DNS Settings Dynamically from WAN

- 3 From the **Name Resolution Method** pull-down menu, select **None**, **DNS**, **NetBios**, or **DNS then NetBios**.
- 4 For **DNS** and **DNS then NetBios**, configure the following DNS settings:
  - **Specify DNS Servers Manually**—Select this radio button to manually configure the DNS servers and specify the IP address(es) in the **Log Resolution DNS Server 1 - 3** fields.
  - **Inherit DNS Settings Dynamically from WAN**—Select this radio button to inherit the DNS settings from the WAN.
- 5 Click **Update**.

# SonicWall Support

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

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 video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- 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

## Legend



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



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



**IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Managements Service System Log Administration  
Updated - January 2023  
232-004554-01 Rev B

## Copyright © 2023 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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. SonicWall Inc. 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/en-us/legal/license-agreements>. Select the language based on your geographic location to see the EUPA that applies to your region.

## Open Source Code

SonicWall 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  
SonicWall Inc. Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035