SonicWall® SonicOS 6.5
Logs and Reporting
Contents

Part 1. Logs & Reporting AppFlow Settings

Managing Flow Reporting Statistics ................................................. 5
Statistics Screen ............................................................................. 6
  External Flow Reporting Statistics ............................................... 7
  Internal AppFlow Reporting Statistics ......................................... 7
  Total IPFIX Statistics .................................................................. 8
Settings Screen ............................................................................... 9
  Settings ....................................................................................... 10
  Local Server Settings ................................................................ 11
  Other Report Settings ................................................................ 11
GMSFlow Server Screen ................................................................. 12
External Collector Screen ............................................................... 14
SFR Mailing Screen ......................................................................... 19
  SFR Email Settings .................................................................... 19
  Scheduling SFR Reports by Email ................................................. 20
Capture Threat Assessment Screen ................................................ 23
NetFlow Activation and Deployment Information .......................... 23
User Configuration Tasks ............................................................... 24
  Configuring NetFlow Version 5 .................................................. 24
  Configuring NetFlow Version 9 .................................................. 25
  Configuring IPFIX (NetFlow Version 10) .................................... 27
  Configuring IPFIX with Extensions ............................................. 28
  Configuring GMSFlow Server to Include Logs via IPFIX ............ 31
  Configuring Netflow with Extensions with SonicWall Scrutinizer ... 32
NetFlow Tables ............................................................................... 35
  Static Tables .............................................................................. 36
  Dynamic Tables ......................................................................... 36
  Templates .................................................................................. 36

Connecting to a GMSFlow Server .................................................... 42
Basic Mode ...................................................................................... 43
Advanced Mode ............................................................................. 44

Part 2. Logs & Reporting Log Settings

Configuring Log Settings ............................................................... 47
Table Columns ............................................................................... 48
Setting Storage Options ............................................................... 51
  Configuring the Storage Module for Log File Storage .................. 52
  Purging a Storage Module ........................................................ 52
Configuring the Log Severity and Priority .................................... 53
  Setting the Logging Level ......................................................... 53
  Setting the Alert Level .............................................................. 54
Configuring Event Attributes Globally ...................................................... 55
Configuring Event Attributes Selectively ............................................... 59
Top Row Buttons ....................................................................................... 61
Viewing and Filtering the Log ................................................................. 63
Adding a Filter .......................................................................................... 64
Viewing a Filter ....................................................................................... 65
Deleting a Filter ...................................................................................... 65

Configuring Syslog Settings ............................................................... 66
About Event Profiles ............................................................................... 67
About Syslog Server Profiling ............................................................... 67
Using a GMS Server for Syslog .............................................................. 68
Syslog Settings ....................................................................................... 68
Syslog Servers ....................................................................................... 71
Adding a Syslog Server ......................................................................... 72
Editing a Syslog Server ......................................................................... 73
Enabling Syslog Servers ....................................................................... 74
Disabling Syslog Servers ...................................................................... 74
Deleting Syslog Servers ....................................................................... 74

Configuring Log Automation .............................................................. 75
Email Log Automation .......................................................................... 76
Health Check E-mail Notification .......................................................... 76
Mail Server Settings ............................................................................. 77
Solera Capture Stack ............................................................................ 78

Configuring Name Resolution ............................................................. 80
Selecting Name Resolution Settings ..................................................... 80
Specifying the DNS Server ................................................................... 80

Configuring the Log Analyzer ............................................................. 81

Configuring AWS Logs ......................................................................... 83
Enabling AWS Logs ............................................................................... 83

Part 3. Logs & Reporting Legal and Support

Accessing Legal Information ................................................................. 86

SonicWall Support ................................................................................ 87
About This Document ........................................................................... 88
Logs & Reporting AppFlow Settings

- Managing Flow Reporting Statistics
- Connecting to a GMSFlow Server
Managing Flow Reporting Statistics

**NOTE:** The AppFlow feature is available on all platforms except SOHO. W.

You manage the firewall's flow reporting, statistics, and configurable settings for sending AppFlow and real-time data to a local collector or external AppFlow servers with the AppFlow feature. AppFlow provides support for external AppFlow reporting formats, such as NetFlow version 5, NetFlow version 9, IPFIX, and IPFIX with Extension. AppFlow includes support for Quest™ Change Auditor for SonicWall, the automated auditing module that allows you to collect data on internet web site and cloud activity. For more information about using Change Auditor with SonicOS firewalls, see [Change Auditor for SonicWall User Guide](#).

The [AppFlow Settings > Flow Reporting](#) page includes settings for configuring the firewall to view statistics based on Flow Reporting and Internal Reporting. From this page, you can also configure settings for internal reporting as well as for GMSflow Server and external collector reporting.

You can access the [AppFlow Reports](#) page by clicking on the [Link](#) icon next to the [Enable Aggregate AppFlow Report Data Collection](#) checkbox of the [AppFlow Settings > Flow Reporting > Settings](#) page.

You can clear the AppFlow settings on each page to their default values by clicking on the [Default Settings](#) button at the bottom of each [AppFlow Settings > Flow Reporting](#) page.
The **AppFlow Settings > Flow Reporting** page has these screens:

- **Statistics** – Displays reporting statistics in four tables
- **Settings** – Allows the enabling of various real-time data collection and AppFlow report collection
- **GMSFlow Server** – Allows the configuring of AppFlow reporting to a GMSFlow server. **External Collector** – Allows
- **External Collector** – Allows the configuring of AppFlow reporting to an IPFIX collector
- **SFR Mailing** – Allows the configuring of the mail servers for the sending the SonicFlow Report (SFR).
- **Capture Threat Assessment** – Allows you to generate and download SFR file.

**Topics:**

- Statistics Screen
- Settings Screen
- GMSFlow Server Screen
- External Collector Screen
- SFR Mailing Screen
- Capture Threat Assessment Screen
- NetFlow Activation and Deployment Information
- User Configuration Tasks
- NetFlow Tables

**Statistics Screen**

This screen displays reports of the flows that are sent to the server, not collected, dropped, stored in and removed from the memory, reported and non-reported to the server. This section also includes the number of NetFlow and IP Flow Information Export (IPFIX) templates sent and general static flows reported.

**Topics:**

- External Flow Reporting Statistics
- Internal AppFlow Reporting Statistics
- Total IPFIX Statistics
External Flow Reporting Statistics

<table>
<thead>
<tr>
<th>External Flow Reporting Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Flows Enqueued:</td>
<td>0</td>
</tr>
<tr>
<td>Connection Flows Dequeued:</td>
<td>0</td>
</tr>
<tr>
<td>Connection Flows Dropped:</td>
<td>0</td>
</tr>
<tr>
<td>Connection Flows Skipped Reporting:</td>
<td>0</td>
</tr>
<tr>
<td>Non-Connection data Enqueued:</td>
<td>596</td>
</tr>
<tr>
<td>Non-Connection data Dequeued:</td>
<td>596</td>
</tr>
<tr>
<td>Non-connection data Dropped:</td>
<td>0</td>
</tr>
<tr>
<td>Non-connection related static data Reported:</td>
<td>0</td>
</tr>
<tr>
<td>Logs Reported by IPFIX:</td>
<td>0</td>
</tr>
</tbody>
</table>

This statistic Displays the total number of
- **Connection Flows Enqueued**: Connection-related flows collected so far.
- **Connection Flows Dequeued**: Connection-related flows that have been reported either to an internal AppFlow collector or external collectors.
- **Connection Flows Dropped**: Collected connection-related flows that failed to get reported.
- **Connection Flows Skipped Reporting**: Connection-related flows that skipped reporting. This can happen when running in periodic mode where collected flows are more than the configured value for reporting.
- **Non-Connection data Enqueued**: All non-connection-related flows that have been collected so far.
- **Non-Connection data Dequeued**: All non-connection-related flows that have been reported either to external collectors or an internal AppFlow collector.
- **Non-connection data Dropped**: All non-connection-related data dropped due to too many requests.
- **Non-connection related static data Reported**: Static non-connection-related static data that have been reported. This includes lists of applications, viruses, spyware, intrusions, table-map, column-map, and location map.
- **Logs Reported by IPFIX**: All logs reported by IPFIX.

Internal AppFlow Reporting Statistics

<table>
<thead>
<tr>
<th>Internal AppFlow Reporting Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Flows Enqueued:</td>
<td>18234</td>
</tr>
<tr>
<td>Data Flows Dequeued:</td>
<td>18254</td>
</tr>
<tr>
<td>Data Flows Dropped:</td>
<td>0</td>
</tr>
<tr>
<td>Data Flows Skipped Reporting:</td>
<td>0</td>
</tr>
<tr>
<td>General Flows Enqueued:</td>
<td>596</td>
</tr>
<tr>
<td>General Flows Dequeued:</td>
<td>596</td>
</tr>
<tr>
<td>General Flows Dropped:</td>
<td>0</td>
</tr>
<tr>
<td>General Static Flows Dequeued:</td>
<td>141306</td>
</tr>
<tr>
<td>AppFlow Collector Errors:</td>
<td>0</td>
</tr>
<tr>
<td>Total Flows in DB:</td>
<td>18233</td>
</tr>
</tbody>
</table>
### Total IPFIX Statistics

The IPFIX statistics are displayed in two tables at the bottom of the Statistics screen.

<table>
<thead>
<tr>
<th>This statistic</th>
<th>Displays the total number of</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total NetFlow/IPFIX Packets Sent</strong></td>
<td>IPFIX/NetFlow packets sent to the all/external collector/AppFlow server/GMSFlow server collected so far.</td>
</tr>
<tr>
<td><strong>NetFlow/IPFIX Packets Sent to External Collection</strong></td>
<td>IPFIX/NetFlow packets sent to the external collector so far.</td>
</tr>
<tr>
<td><strong>Netflow/IPFIX Packets Sent to GMSFlow Server</strong></td>
<td>IPFIX/NetFlow packets sent to the GMSFlow collector so far.</td>
</tr>
<tr>
<td><strong>NetFlow/IPFIX Templates Sent</strong></td>
<td>IPFIX/NetFlow templates sent to the all/external collector/AppFlow server/GMSFlow serve.</td>
</tr>
<tr>
<td><strong>Connection Flows Sent to External Collector</strong></td>
<td>Connection/static/general flows that have been reported to the external collector.</td>
</tr>
<tr>
<td><strong>Connection Flows Sent to GMSFlow Server</strong></td>
<td>Connection/static/general flows that have been reported to the GMSFlow server.</td>
</tr>
<tr>
<td><strong>Non-Connection related Dynamic Flows Sent to External Collector:</strong></td>
<td>IPFIX/netflow packets sent to the external collector so far.</td>
</tr>
</tbody>
</table>

---

### Total IPFIX Statistics

<table>
<thead>
<tr>
<th>Total IPFIX Statistics</th>
<th>Total IPFIX Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total NetFlow/IPFIX Packets Sent</td>
<td>0</td>
</tr>
<tr>
<td>NetFlow/IPFIX Packets Sent to External Collection</td>
<td>0</td>
</tr>
<tr>
<td>Netflow/IPFIX Packets Sent to GMSFlow Server</td>
<td>0</td>
</tr>
<tr>
<td>NetFlow/IPFIX Templates Sent</td>
<td>0</td>
</tr>
<tr>
<td>Connection Flows Sent to External Collector</td>
<td>0</td>
</tr>
<tr>
<td>Connection Flows Sent to GMSFlow Server</td>
<td>0</td>
</tr>
<tr>
<td>Non-Connection related Dynamic Flows Sent to External Collector</td>
<td>0</td>
</tr>
</tbody>
</table>
Settings Screen

The Settings screen has configurable options for local internal flow reporting, AppFlow Server external flow reporting, and the IPFIX collector.

<table>
<thead>
<tr>
<th>This statistic</th>
<th>Displays the total number of</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Connection related Dynamic Flows Sent to GMSFlow Server</td>
<td>IPFIX/netflow packets sent to the GMSFlow server so far.</td>
</tr>
<tr>
<td>Non-Connection related Static Flows Sent to External Collector</td>
<td>Connection/static/general flows that have been reported to the AppFlow collector or external collector.</td>
</tr>
<tr>
<td>Logs Reported by IPFIX to external collector</td>
<td>Logs reported to the external collector by IPFIX so far.</td>
</tr>
<tr>
<td>Non-Connection related Static Flows Sent to GMSFlow Server</td>
<td>Connection/static/general flows that have been reported to the GMSFlow server.</td>
</tr>
<tr>
<td>Logs Reported by IPFIX to GMSFlow Server</td>
<td>Logs reported to the GMSFlow server by IPFIX so far.</td>
</tr>
</tbody>
</table>

The Settings screen has three sections:

- **Settings**
- **Local Server Settings**
- **Other Report Settings**
Settings

The Settings section of the Settings screen allows you to enable real-time data collection and AppFlow report collection.

- **Report Collections**—Enables AppFlow reporting collection according to one of these modes:
  - **All** — Selecting this checkbox reports all flows. This is the default setting.
  - **Interface-based** — Selecting this checkbox enables flow reporting based only on the initiator or responder interface. This provides a way to control what flows are reported externally or internally. If enabled, the flows are verified against the per interface flow reporting configuration, located in the Network > Interfaces page.

    If an interface has its flow reporting disabled, then flows associated with that interface are skipped.

  - **Firewall/App Rules-based** — Selecting this checkbox enables flow reporting based on already existing firewall Access and App rules configuration, located on the Firewall > Access Rules page and the Firewall > App Rules page, respectively. This is similar to interface-based reporting; the only difference is instead of checking per interface settings, the per-firewall rule is selected.

    Every firewall Access and App rule has a checkbox to enable flow reporting. If a flow matching a rule is to be reported, this enabled checkbox forces verification that firewall rules have flow reporting enabled or not.

    **NOTE:** If this option is enabled, but no rules have the flow-reporting option enabled, no data is reported. This option is an additional way to control which flows need to be reported.

- **Enable Real-Time Data Collection**—Enables real-time data collection on your firewall for real-time statistics. You can enable/disable individual items in the Collect Real-Time Data For drop-down menu. This setting is enabled by default.

    When this setting is disabled, the Real-Time Monitor does not collect or display streaming data as the real-time graphs displayed in the MONITOR > Appliance Health > Live Monitor page are disabled.

- **Collect Real-Time Data For**—Select the streaming graphs to display on the Real-Time Monitor page. By default, all items are selected.

    | This option          | Displays this graph(s)               |
    |----------------------|--------------------------------------|
    | Top apps             | Applications                         |
    | Bits per sec.        | Bandwidth                            |
    | Packets per sec.     | Packet Rate                          |
    | Average packet size  | Packet Size                          |
    | Connections per sec. | Connection Rate and Connection Count |
    | Core util.           | Multi-Core Monitor                   |
    | Memory util.         | Memory Usage                         |

SonicWall SonicOS 6.5 Logs and Reporting
Managing Flow Reporting Statistics
• **Enable Aggregate AppFlow Report Data Collection**—Enables individual AppFlow Reports collection on your SonicWall appliance for display in INVESTIGATE | Reports | AppFlow Reports. You can enable/disable Individual items in the Collect Report Data For drop-down menu. This setting is enabled by default.

When this setting is disabled, the AppFlow Reports does not collect or display data.

**TIP:** You can quickly display the INVESTIGATE | Reports | AppFlow Reports page by clicking the Display icon by the Enable Aggregate AppFlow Report Data Collection checkbox.

• **Collect Report Data For**—Select from this drop-down menu the data to display on the INVESTIGATE | Reports | AppFlow Reports page. By default, all reports are selected.

  • Apps Report
  • User Report
  • IP Report
  • Threat Report
  • Geo-IP Report
  • URL Report

**Local Server Settings**

The Local Server Settings section allows you to enable AppFlow reporting to an internal collector.

Selecting Enable AppFlow To Local Collector enables AppFlow reporting collection to an internal server on your SonicWall appliance. If this option is disabled, the tabbed displays on INVESTIGATE | Reports | AppFlow Reports are disabled. By default, this option is disabled.

**NOTE:** When enabling/disabling this option, you may need to reboot the device to enable/disable this feature completely.

**Other Report Settings**

The options in the Other Report Settings section configure conditions under which a connection is reported. This section does not apply to all non-connection-related flows.

• **Report DROPPED Connection**—If enabled, connections that are dropped due to firewall rules are not reported. This option is enabled by default.

• **Skip Reporting STACK Connections**—If enabled, the firewall will not report all connections initiated or responded to by the firewall’s TCP/IP stack. By default, this option is enabled.
• **Include Following URL Types**—From the drop-down menu, select the type of URLs that need to be reported. To skip a particular type of URL reporting, uncheck (disable) them.

  ![NOTE: This setting applies to both AppFlow reporting (internal) and external reporting when using IPFIX with extensions.]

  - Gifs (selected by default)
  - Jpegs (selected by default)
  - Pngs (selected by default)
  - Js
  - Xmls
  - Jsons
  - Css
  - Htmls (selected by default)
  - Aspx (selected by default)

• **Enable Geo-IP Resolution**—Enables Geo-IP resolution. If disabled, the AppFlow Monitor does not group flows based on country under Initiators and Responders tabs. This setting is unchecked (disabled) by default.

  ![NOTE: If Geo-IP blocking or Botnet blocking is enabled, this option is ignored.]

• **Disable Reporting IPv6 Flows (ALL)**—Disables reporting of IPv6 flows. This setting is enabled by default.

• **AppFlow Report Upload Timeout (sec)**—Specify the timeout, in seconds, when connecting to the AppFlow upload server. The minimum timeout is 5 seconds, the maximum is 300 seconds, and the default value is **120** seconds.

### GMSFlow Server Screen

This screen provides configuration settings for sending AppFlow and Real-Time data to a GMSFlow server.

- **Send AppFlow to SonicWall GMSFlow Server** – The SonicWall appliance sends AppFlow data via IPFIX to a SonicWall GMSFlow server. This option is not enabled by default.

  If this option is disabled, the SonicWall GMSFlow server does not show AppFlow Monitor, AppFlow Report, and AppFlow Dashboard charts on the GMSFlow server or via redirection an another SonicWall appliance.

  ![NOTE: When enabling/disabling this option, you may need to reboot the device to enable/disable this feature completely.]

SonicWall SonicOS 6.5 Logs and Reporting
Managing Flow Reporting Statistics
• **Send Real-Time Data to SonicWall GMSFlow Server** – The SonicWall appliance sends real-time data via IPFIX to the SonicWall GMSFlow server. This option is disabled by default.

If this option is disabled, the SonicWall GMSFlow server does not display real-time charts on the GMSFlow server or via redirection on a SonicWall appliance.

• **Send System Logs to SonicWall GMSFlow Server** – The SonicWall firewall sends system logs via IPFIX to the SonicWall GMSFlow server. This option is not selected by default.

• **Report on Connection OPEN** – The SonicWall appliance reports when a new connection is opened. All associated data related to that connection may not be available when the connection is opened. This option enables flows to show up on the GMSFlow server as soon as a new connection is opened. This option is disabled by default.

• **Report on Connection CLOSE** – The SonicWall appliance reports when a new connection is closed. This is the most efficient way of reporting flows to the GMSFlow server. All associated data related to that connection are available and reported. This option is enabled by default.

• **Report Connections on Following Updates** – The firewall reports when a specified update occurs. Select the updates from the drop-down menu. By default, no update is selected.

  threat detection
  application detection
  user detection
  VPN tunnel detection
  URL detection

• **Send Dynamic AppFlow For Following Tables** – The firewall sends data for the selected tables. By default, all the tables are selected.

  Connections
  Users
  URLs
  URL ratings
  VPNs
  Devices
  SPAMs
  Locations
  VOIPs

**IMPORTANT:** In IPFIX with extension mode, the firewall can generate reports for selected tables. As the firewall doesn’t cache this data, some of the flows not sent may create failure when correlating flows with other, related data.
External Collector Screen

The **External Collector** screen provides configuration settings for AppFlow reporting to an external IPFIX collector.

- **Send Flows and Real-Time Data To External Collector**—Enables the specified flows to be reported to an external flow collector. This option is disabled by default.

  **IMPORTANT:** When enabling/disabling this option, you may need to reboot the device to enable/disable this feature completely.

- **External AppFlow Reporting Format**—If the **Report to EXTERNAL Flow Collector** option is selected, you must select the flow-reporting type from the drop-down menu:
  - **NetFlow version-5** (default)
  - **NetFlow version-9**
  - **IPFIX**
  - **IPFIX with extensions**

  1. IPFIX with extensions v2 is still supported by enabling an internal setting. For how to enable this option, contact **SonicWall Support**. Currently, GMSFlow Server does not support this IPFIX version.

  **NOTE:** Your selection for **External Flow Reporting Format** changes the available options.

If the reporting type is set to:
- **Netflow** versions 5 or 9 or **IPFIX**, then any third-party collector can be used to show flows reported from the firewall, which uses standard data types as defined in IETF. **Netflow** versions and **IPFIX** reporting types contain only connection-related flow details per the standard.
• **IPFIX with extensions**, then only collectors that are SonicWall-flow aware can be used to report SonicWall dynamic tables for:

<table>
<thead>
<tr>
<th>connections</th>
<th>users</th>
<th>applications</th>
<th>locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>URLs</td>
<td>logs</td>
<td>devices</td>
<td>VPN tunnels</td>
</tr>
<tr>
<td>devices</td>
<td>SPAMs</td>
<td>wireless</td>
<td>real-time health (memory/CPU/face statistics)</td>
</tr>
</tbody>
</table>

Flows reported in this mode can either be viewed by another SonicWall firewall configured as a collector (specially in a High Availability pair with the idle firewall acting as a collector) or a SonicWall Linux collector. Some third-party collectors also can use this mode to display applications if they use standard IPFIX support. Not all reports are visible when using a third-party collector, though.

**NOTE:** When using **IPFIX with extensions**, select a third-party collector that is SonicWall-flow aware, such as Scrutinizer.

• **External Collector’s IP Address**—Specify the external collector’s IP address to which the device sends flows via Netflow/IPFIX. This IP address must be reachable from the SonicWall firewall for the collector to generate flow reports. If the collector is reachable via a VPN tunnel, then the source IP must be specified in **Source IP to Use for Collector on a VPN Tunnel**.

• **Source IP to Use for Collector on a VPN Tunnel**—If the external collector must be reached by a VPN tunnel, specify the source IP for the correct VPN policy.

  **NOTE:** Select Source IP from the local network specified in the VPN policy. If specified, Netflow/IPFIX flow packets always take the VPN path.

• **External Collector’s UDP Port Number**—Specify the UDP port number that Netflow/IPFIX packets are being sent over. The default port is 2055.

• **Send IPFIX/Netflow Templates at Regular Intervals**—Enables the appliance to send Template flows at regular intervals. This option is selected by default.

  **NOTE:** This option is available with **Netflow version-9, IPFIX, IPFIX with extensions** only.

Netflow version-9 and IPFIX use templates that must be known to an external collector before sending data. Per IETF, a reporting device must be capable of sending templates at a regular interval to keep the collector in sync with the device. If the collector does not need templates at regular intervals, you can disable the function here.

• **Send Static AppFlow at Regular Interval**—Enables the hourly sending of IPFIX records for the specified static appflows tables. This option is disabled by default.

  **NOTE:** This option is available with **IPFIX with extensions** only. This option **must** be selected if SonicWall Scrutinizer is used as a collector.

• **Send Static AppFlow for Following Tables**—Select the static mapping tables to be generated to a flow from the drop-down menu. For more information on static tables, refer to **NetFlow Tables**.

  - **Applications** (selected by default)
  - **Services** (selected by default)
  - **Viruses** (selected by default)
  - **Rating Map** (selected by default)
  - **Spyware** (selected by default)
  - **Table Map**
  - **Intrusions** (selected by default)
  - **Column Map**
  - **Location Map**
When running in **IPFIX with extensions** mode, the firewall reports multiple types of data to an external device to correlate User, VPN, Application, Virus, and Spyware information. Data is both static and dynamic. Static tables are needed only once as they rarely change. Depending on the capability of the external collector, not all static tables are needed.

In the **IPFIX with extension** mode, the firewall can asynchronously generate the static mapping table(s) to synchronize the external collector. This synchronization is needed when the external collector is initialized later than the firewall.

- **Send Dynamic AppFlow for Following Tables**—Select the dynamic mapping tables to be generated to a flow from the drop-down menu. For more information on dynamic tables, refer to NetFlow Tables.

  **NOTE:** This option is available with **IPFIX with extensions** only.

  The firewall generates reports for the selected tables. As the firewall doesn’t cache this information, some of the flows not sent may create failure when correlating flows with other related data.

<table>
<thead>
<tr>
<th>Connections (selected by default)</th>
<th>Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users (selected by default)</td>
<td>SPAMs</td>
</tr>
<tr>
<td>URLs (selected by default)</td>
<td>Locations</td>
</tr>
<tr>
<td>URL ratings (selected by default)</td>
<td>VoIPs (selected by default)</td>
</tr>
<tr>
<td>VPNs (selected by default)</td>
<td></td>
</tr>
</tbody>
</table>

- **Include Following Additional Reports via IPFIX**—Select additional IPFIX reports to be generated to a flow. Select values from the drop-down menu. By default, none are selected. Statistics are reported every 5 seconds.

  **NOTE:** This option is available with **IPFIX with extensions** only.

  - **System Logs**—Generates system logs such as interface state change, fan failure, user authentication, HA failover and failback, tunnel negotiations, configuration change. System logs include events that are typically not flow-related (session/connection) events, that is, not dependent on traffic flowing through the firewall.
  - **Top 10 Apps**—Generates the top 10 applications.
  - **Interface Stats**—Generates per-interface statistics such as interface name, interface bandwidth utilization, MAC address, link status.
  - **Core utilization**—Generates per-core utilization.
  - **Memory utilization**—Generates statuses of available memory, used memory, and memory used by the AppFlow collector.

When running in either mode, SonicWall can report more data that is not related to connection and flows. These tables are grouped under this section (Additional Reports). Depending on the capability of the external collector, not all additional tables are needed. With this option, you can select tables that are needed.

- **Report On Connection OPEN**—Reports flows when a new connection is established. All associated data related to that connection may not be available when the connection is opened. This option, however, enables flows to show up on the external collector as soon as the new connection is established. By default, this setting is enabled.

- **Report On Connection CLOSE**—Reports flows when a connection is closed. This is the most efficient way of reporting flows to an external collector. All associated data related to that connection are available and reported. By default, this setting is enabled.
• **Report Connection On Active Timeout**—Reports connections based on Active Timeout sessions. If enabled, the firewall reports an active connection every active timeout period. By default, this setting is disabled.

  **NOTE:** If you select this option, the Report Connection On Kilo BYTES Exchanged option cannot be selected also. If this option is already checked, this message is displayed when attempting to select Report Connection on Kilo BYTES Exchanged:

  ![Message]

• **Number of Seconds**—Set the number of seconds to elapse for the Active Timeout. The range is 1 second to 999 seconds for the Active Timeout. The default setting is 60 seconds.

• **Report Connection On Kilo BYTES Exchanged**—Reports flows based on when a specific amount of traffic, in kilobytes, is exchanged. If this setting is enabled, the firewall reports an active connection whenever the specified number of bytes of bidirectional data is exchanged on an active connection. This option is ideal for flows that are active for a long time and need to be monitored. This option is not selected by default.

  **NOTE:** If you select this option, the Report Connection On Active Timeout option cannot be selected also. If this option is already checked, this message is displayed when attempting to select Report Connection on Active Timeout:

  ![Message]

• **Kilobytes Exchanged**—Specify the amount of data, in kilobytes, transferred on a connection before reporting. The default value is 100 kilobytes.

• **Report ONCE**—When the Report Connection On Kilo BYTES Exchanged option is enabled, the same flow is reported multiple times whenever the specified amount of data is transferred over the connection. This could cause a large amount of IPFIX-packet generation on a loaded system. Enabling this option sends the report only once. This option is selected by default.

• **Report Connections On Following Updates**—Select from the pull-down menu to enable connection reporting for the following (by default, all are selected):

<table>
<thead>
<tr>
<th>This selection</th>
<th>Reports flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>threat detection</td>
<td>Specific to threats. Upon detections of virus, intrusion, or spyware, the flow is reported again.</td>
</tr>
<tr>
<td>application detection</td>
<td>Specific to applications. Upon performing a deep packet inspection, the SonicWall appliance is able to detect if a flow is part of a certain application. When identified, the flow is reported again.</td>
</tr>
<tr>
<td>user detection</td>
<td>Specific to users. The SonicWall appliance associates flows to a user-based detection based on its login credentials. When identified, the flow is reported again.</td>
</tr>
<tr>
<td>VPN tunnel detection</td>
<td>Sent through the VPN tunnel. When flows sent over the VPN tunnel are identified, the flow is reported again.</td>
</tr>
</tbody>
</table>

• **Actions**—Generate templates and static flow data asynchronously when you click these buttons:
• **Generate ALL Templates** — Click on the button to begin building templates on the IPFIX server; this takes up to two minutes to generate.  
  
  **NOTE:** This option is available with Netflow version-9, IPFIX, and IPFIX with extensions only.

• **Generate Static AppFlow Data** — Click on the button to begin generating a large amount of flows to the IPFIX server; this takes up to two minutes to generate.  
  
  **NOTE:** This option is available with IPFIX with extensions only.

• **Log Settings To External Collector** – Sends the necessary fields of log settings to the external collector when you click the Send All Entries button.  
  
  **TIP:** This option displays only when IPFIX with extensions is selected for External Flow Reporting Format.  
  
  **NOTE:** Ensure the connection between SonicOS and the external collector server is ready before clicking the Send All Entries button.  
  
  **TIP:** Click the button again to sync the settings whenever:  
  • SonicOS is upgraded with new added log events.  
  • The connection between SonicOS and the external server has been down for some time and log settings may have been edited.
SFR Mailing Screen

Use SFR Mailing screen to have your SonicFlow Report (SFR) automatically sent to an Email address.

Topics:
- SFR Email Settings
- Scheduling SFR Reports by Email

SFR Email Settings

To automatically send your SonicFlow Report (SFR) to an Email address:

2. Click the SFR Mailing tab.
3. Select the Send Report by E-mail checkbox.
4. Enter these options:
   - The address of the email server in the SMTP Server Host Name field.
   - The recipient’s email address in the E-mail To field.
   - The email address used for the sender in the From E-mail field.
• The SMTP port number in the **SMTP Port** field. The default value is **25**.

• A security method for the email from the **Connection Security Method** drop-down menu:
  - **None** (default)
  - **SSL/TLS**
  - **STARTTLS**

5 If your email server requires SMTP authentication, select the **Enable SMTP Authentication** checkbox and enter these options:
  - User name in the **SMTP User Name** field
  - Password in the **SMTP User Password** field

6 If your email server supports POP Before SMTP authentication, you can select the **POP Before SMTP** checkbox and enter these options:
  - Address of the POP server in the **POP Server Address** field.
  - User name in the **POP User Name** field
  - Password in the **POP User Password** field.

7 Click **Accept**.

**To test the Email settings:**

1 Enter the required values in the **SFR Email Settings**.

2 Click **Test Email**.

   • If the Email settings are correct, a confirmation dialog box is displayed.
   • If the Email settings are incorrect, a warning dialog box is displayed:

```
Failed to initiate the test email [2]
```

   You will need to verify the Email settings and try again.

**Scheduling SFR Reports by Email**

You can schedule the report to be sent one time, on a recurring schedule, or both.

**You can configure the delivery schedule for the report:**

1 Navigate to **MANAGE | Logs & Report > Appflow Settings > Flow Reporting**.

2 Click the **SFR Mailing** tab.

3 Select the **Send Report by E-mail** checkbox.

4 In the **Schedule Email Sending** section, click the **Edit Schedule** button to schedule how when the SonicFlow Report (CFR) is sent by Email.

5 The **Add Schedule** dialog box appears:
6 In the **Schedule Name** field, enter a name for your report.

7 Select how often you want the report sent:
   - **Once** – Send the report one time at the specified date and time.
   - **Recurring** – Send the report on a recurring basis on the specified days and time.
   - **Mixed** – Send the report one time and on a recurring basis on the specified days and time.

**Topics:**
- Scheduling One-Time Delivery of the SFR
- Scheduling Recurring Delivery of the SFR

**Scheduling One-Time Delivery of the SFR**

*To schedule one-time delivery of the SonicFlow Report (SFR):*

1. For the **Schedule type**, select **Once**.

2. In the **Once** section, set the duration for which you want the SFR to be created. Select the Year, Month, Day, Hour, and Minute from the drop-down menus to set the Start and End period for the report.

3. Click **OK**.
Scheduling Recurring Delivery of the SFR

To schedule recurring delivery of the SonicFlow Report (SFR):

1. For the Schedule type, select Recurring.

2. In the Recurring section:
   a. Select the days for which you want the report created. Click All to select all of the days at once.
   b. Enter the Start Time and Stop Time for the report in 24-hour format (for example, 02:00 for 2:00am and 14:00 for 2:00pm).
   c. Click Add to add that report to the Schedule List.
   d. Repeat these steps for each scheduled report you want to create.

3. Click OK.

Deleting Scheduled Reports

You can delete any or all scheduled reports.

To delete selected scheduled reports:

1. Select the reports to be deleted in the Schedule List.
2. Click Delete. The reports you selected will be deleted from the list.
3. Click OK.

To delete all scheduled reports:

1. Click Delete All. All of the reports will be deleted from the list.
2. Click OK.
Capture Threat Assessment Screen

Use the Capture Threat Assessment screen to generate a SonicFlow Report (SFR) that you can download and post to the Capture Threat Assessment service.

To generate and post the SonicFlow Report (SFR):

2. Click Generate Report.
3. After the report is generated, you will have the option to download the report or generate a new one.
4. Click Download Report to download the report.

NetFlow Activation and Deployment Information

SonicWall recommends careful planning of NetFlow deployment with NetFlow services activated on strategically located edge/aggregation routers which capture the data required for planning, monitoring and accounting applications. Key deployment considerations include the following:

- Understanding your application-driven data collection requirements: accounting applications may only require originating and terminating router flow information whereas monitoring applications may require a more comprehensive (data intensive) end-to-end view
• Understanding the impact of network topology and routing policy on flow collection strategy: for example, avoid collecting duplicate flows by activating NetFlow on key aggregation routers where traffic originates or terminates and not on backbone routers or intermediate routers which would provide duplicate views of the same flow information.

• NetFlow can be implemented in the SonicOS management interface to understand the number of flow in the network and the impact on the router. NetFlow export can then be setup at a later date to complete the NetFlow deployment.

NetFlow is, in general, an ingress measurement technology which should be deployed on appropriate interfaces on edge/aggregation or WAN access routers to gain a comprehensive view of originating and terminating traffic to meet customer needs for accounting, monitoring or network planning data. The key mechanism for enhancing NetFlow data volume manageability is careful planning of NetFlow deployment. NetFlow can be deployed incrementally (that is, interface by interface) and strategically (that is, on well-chosen routers) — instead of widespread deployment of NetFlow on every router in the network.

User Configuration Tasks

Depending on the type of flows you are collecting, you will need to determine which type of reporting works best with your setup and configuration. This section includes configuration examples for each supported NetFlow solution, as well as configuring a second appliance to act as a collector.

• Configuring NetFlow Version 5
• Configuring NetFlow Version 9
• Configuring IPFIX (NetFlow Version 10)
• Configuring IPFIX with Extensions
• Configuring GMSFlow Server to Include Logs via IPFIX
• Configuring Netflow with Extensions with SonicWall Scrutinizer

Configuring NetFlow Version 5

To configure Netflow version 5 flow reporting:

1 Click Settings.

   | Statistics | Settings | GMSFlow Server | External Collector | SIP Mailing | Capture Threat Assessment |

2 For Report Connections in the Settings section, select one of these radio buttons:

• All (default)
• Interface-based: when enabled, the flows reported are based on the initiator or responder interface.
• Firewall/App Rules-based: when enabled, the flows reported are based on already existing firewall rules.

When enabled, the flows reported are based on the initiator or responder interface or on already existing firewall rules.

   NOTE: This step is optional, but is required if flow reporting is done on selected interfaces.
3 Click the **External Collector** screen.

4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

5 Select **Netflow version-5** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector’s IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

   **IMPORTANT:** This step is required if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector’s UDP port number** in the provided field. The default port is **2055**.

9 Click the **Accept** button at the top of the page.

   **NOTE:** You may need to reboot the device to completely enable this configuration.

### Configuring NetFlow Version 9

**To configure Netflow version 9 flow reporting:**

1 Click Settings.
2 In the Settings section, for Report Connections, select one of these radio buttons:
  
  - **All** (default)
  - **Interface-based**: when enabled, the flows reported are based on the initiator or responder interface.
  - **Firewall/App Rules-based**: when enabled, the flows reported are based on already existing firewall rules.

  **IMPORTANT:** This step is optional, but is required if flow reporting is done on selected interfaces.

3 Click External Collector.

4 Select the **Send Flows and Real-Time Data To External Collector** checkbox.

  **IMPORTANT:** When enabling this option, you may need to reboot the device to enable this feature completely.

5 Select **Netflow version-9** as the **External Flow Reporting Format** from the drop-down menu.

6 Specify the **External Collector’s IP address** in the provided field.

7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

  **IMPORTANT:** This step is required if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector’s UDP port number** in the provided field. The default port is **2055**.

9 In **Actions**, click the **Generate ALL Templates** button to begin generating templates. A message requesting confirmation displays.

  **IMPORTANT:** IPFIX uses templates that must be known to an external collector before sending data.
10 After the templates have been generated, click Accept.

Configuring IPFIX (NetFlow Version 10)

To configure IPFIX, or NetFlow version 10, flow reporting:

1. Click Settings.

2. In the Settings section, for Report Connections, select one of these radio buttons:
   - All (default)
   - Interface-based: when enabled, the flows reported are based on the initiator or responder interface.
   - Firewall/App Rules-based: when enabled, the flows reported are based on already existing firewall rules.

   IMPORTANT: This step is optional, but is required if flow reporting is done on selected interfaces.

3. Click External Collector.
4 Select the Send Flows and Real-Time Data To External Collector checkbox.

**IMPORTANT:** When enabling this option, you may need to reboot the device to enable this feature completely.

5 Select IPFIX as the External Flow Reporting Format from the drop-down menu.

6 Specify the External Collector’s IP address in the provided field.

7 Optionally, for the Source IP to Use for Collector on a VPN Tunnel, specify the source IP if the external collector must be reached by a VPN tunnel.

**IMPORTANT:** This step is required if the external collector must be reached by a VPN tunnel.

8 Specify the External Collector’s UDP port number in the provided field. The default port is 2055.

9 In Actions, click the Generate ALL Templates button to begin generating templates. A message requesting confirmation displays.

**IMPORTANT:** IPFIX uses templates that must be known to an external collector before sending data.

10 After the templates have been generated, click Accept.

### Configuring IPFIX with Extensions

To configure IPFIX with extensions flow reporting:

1 Click Settings.

**IMPORTANT:** Enabling or disabling features marked with * may require a reboot.

2 In the Settings section, for Report Connections, select one of these radio buttons:

- **All** (default)
- **Interface-based**: when enabled, the flows reported are based on the initiator or responder interface.
- **Firewall/App Rules-based**: when enabled, the flows reported are based on already existing firewall rules.

**IMPORTANT:** This step is optional, but is required if flow reporting is done on selected interfaces.
3. Click **External Collector**.

4. Select the **Send Flows and Real-Time Data To External Collector** checkbox.
   - **IMPORTANT**: When enabling this option, you may need to reboot the device to enable this feature completely.

5. Select **IPFIX with extensions** as the **External Flow Reporting Format** from the drop-down menu.

6. Specify the **External Collector’s IP address** in the provided field.

7. For the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.
   - **IMPORTANT**: This step is required if the external collector must be reached by a VPN tunnel.

8. Specify the **External Collector’s UDP port number** in the provided field. The default port is **2055**.

9. Select the tables you wish to receive static flows for from the **Send Static AppFlow For Following Tables** drop-down menu.

10. Select the tables you wish to receive dynamic flows for from the **Send Dynamic AppFlow For Following Tables** drop-down menu.

11. Select any additional reports to be generated to a flow from the **Include Following Additional Reports via IPFIX** drop-down menu.
    - **IMPORTANT**: To have system logs generated, you must select System Logs from this drop-down menu.

12. Click the **Generate ALL Templates** button to begin generating templates.
    - **IMPORTANT**: IPFIX with extensions uses templates that must be known to an external collector before sending data.
13 Enable the option to **Send Static AppFlow at Regular Intervals** by selecting the checkbox. After enabling this option, click the **Generate Static Flows** button.

![Message dialog](image)

14 To begin generating static flow data, click the **Generate Static AppFlow Data** button. A message requesting confirmation displays.

![Message dialog](image)

15 To send log messages to the external collector, click the **Send All Entries** button for the **Send Log Settings to External Collector** option.

**IMPORTANT:** Ensure the connection between SonicOS on the firewall and the external collector server is ready before clicking the **Send All Entries** button.

The external server loads the properties (see **Saved properties**) and settings for use when it reboots. Click the **Send All Entries** button to synchronize the settings whenever:

- SonicOS is upgraded, for example, with new log events.
- The connection between SonicOS (firewall) and the external server has been down for some time and log settings may have been edited during that time.

**NOTE:** SonicOS sends updates to the external server automatically if some fields of log event settings are changed.

**Saved properties**

<table>
<thead>
<tr>
<th>Category</th>
<th>Property</th>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event properties and settings</td>
<td>Event ID</td>
<td>Priority</td>
</tr>
<tr>
<td></td>
<td>Belongs to group ID</td>
<td>Stream filter</td>
</tr>
<tr>
<td></td>
<td>Color</td>
<td>Event name</td>
</tr>
<tr>
<td></td>
<td>Message type ID</td>
<td>Log message</td>
</tr>
<tr>
<td>Group properties</td>
<td>Group ID</td>
<td>Group name</td>
</tr>
<tr>
<td></td>
<td>Belongs to category ID</td>
<td></td>
</tr>
<tr>
<td>Category properties</td>
<td>Category ID</td>
<td>Category name</td>
</tr>
<tr>
<td>Message type properties</td>
<td>Type ID</td>
<td>Type name</td>
</tr>
</tbody>
</table>

16 Click **Accept**.
Configuring GMSFlow Server to Include Logs via IPFIX

To configure GMSFlow server to include logs via IPFIX:


2. Click GMSFlow Server.

3. Select the Send System Logs to SonicWall GMSFlow Server checkbox. This option is not selected by default.

4. Click Accept.
5 Navigate to AppFlow Settings > GMS Flow Server.

6 To send log messages to the GMSFlow server, click the Synchronize Log Settings button.
   - **IMPORTANT:** Ensure the connection between SonicOS on the firewall and the GMSFlow server is ready before clicking the Synchronize Log Settings button.

   The external server loads the properties (see Saved properties) and settings for use when it reboots. Click the Send All Entries button to synchronize the settings whenever:
   - SonicOS is upgraded, for example, with new log events.
   - The connection between SonicOS (firewall) and the external server has been down for some time and log settings may have been edited during that time.
   - **NOTE:** SonicOS sends updates to the external server automatically if some fields of log event settings are changed.

7 Click Accept.

**Configuring Netflow with Extensions with SonicWall Scrutinizer**

One external flow reporting option that works with Netflow with Extensions is the third-party collector, SonicWall Scrutinizer. This collector displays a range of reporting and analysis that is both Netflow and SonicWall-flow aware.

**To verify your Netflow with Extensions reporting configurations:**

1 Click Settings.

2 In the Settings section, for Report Connections, select the All radio button.
   - **IMPORTANT:** This step is optional, but is required if flow reporting is done on selected interfaces.

3 Click External Collector.
4 Click the **Send Flows and Real-Time Data To External Collector** checkbox.  

   **IMPORTANT:** When enabling this option, you may need to reboot the device to enable this feature completely.

5 Select **IPFIX with extensions** from the **External Flow Reporting Format** drop-down menu.

6 Specify the **External Collector’s IP address** in the provided field.

7 Optionally, if the external collector must be reached by a VPN tunnel, specify the source IP in the **Source IP to Use for Collector on a VPN Tunnel** field.

   **IMPORTANT:** This step is *required* if the external collector must be reached by a VPN tunnel.

8 Specify the **External Collector’s UDP port number** in the provided field. The default port is **2055**.

9 Click the **Send Static AppFlow At Regular Interval** checkbox.

10 Select the tables you wish to receive static flows for from the **Send Dynamic AppFlow For Following Tables** drop-down menu.
11 Click the **Generate Static AppFlow Data** button.

12 Click **Accept**.

13 Navigate to **System Setup | Network > Interfaces**.

14 Confirm that Flow Reporting is enabled per interface by clicking the **Configure** icon of the interface you are requesting data from. The **Edit Interface** dialog displays.
15 On the Advanced screen, ensure the checkbox to Enable flow reporting is selected.

![Advanced Settings](image)

16 Click OK.
17 Login to SonicWall Scrutinizer. The data displays within minutes.

![SonicWall Scrutinizer](image)

**NetFlow Tables**

The following section describes the various NetFlow tables. Also, this section describes in detail the IPFIX with extensions tables that are exported when the SonicWall is configured to report flows.

**Topics:**
- Static Tables
- Dynamic Tables
- Templates
  - NetFlow Version 5
  - NetFlow Version 9
  - IPFIX (NetFlow Version 10)
  - IPFIX with Extensions
Static Tables

Static Tables are tables with data that does not change over time. However, this data is required to correlate with other tables. Static tables are usually reported at a specified interval, but may also be configured to send just once. Exportable Static IPFIX tables lists the Static IPFIX tables that may be exported:

Exportable Static IPFIX tables

- **Applications Map** Reports all applications the firewall identifies, including various Attributes, Signature IDs, App IDs, Category Names, and Category IDs.
- **Viruses Map** Reports all viruses detected by the firewall.
- **Spyware Map** Reports all spyware detected by the firewall.
- **Intrusions Map** Reports all intrusions detected by the firewall.
- **Location Map** Represents SonicWall's location map describing the list of countries and regions with their IDs.
- **Services Map** Represents SonicWall's list of Services with Port Numbers, Protocol Type, Range of Port Numbers, and Names.
- **Rating Map** Represents SonicWall's list of Rating IDs and the Name of the Rating Type.
- **Table Layout Map** Reports SonicWall's list of tables to be exported, including Table ID and Table Names.
- **Column Map** Represents SonicWall's list of columns to be reported with Name, Type Size, and IPFIX Standard Equivalents for each column of every table.

Dynamic Tables

Unlike Static tables, the data of Dynamic tables change over time and are sent repeatedly, based on the activity of the firewall. The columns of these tables grow over time, with the exception of a few tables containing statistics or utilization reports. Exportable Dynamic IPFIX tables lists the Dynamic IPFIX tables that may be exported:

Exportable Dynamic IPFIX tables

- **Connections** Reports SonicWall connections. The same flow tables can be reported multiple times by configuring triggers.
- **Users** Reports users logging in to the firewall via LDAP/RADIUS, Local, or SSO.
- **URLs** Reports URLs accessed through the firewall.
- **URL ratings** Reports Rating IDs for all URLs accessed through the firewall.
- **VPNs** Reports all VPN tunnels established through the firewall.
- **Devices** Reports the list of all devices connected through the firewall, including the MAC addresses, IP addresses, Interface, and NETBIOS name of connected devices.
- **SPAMs** Reports all email exchanges through the SPAM service.
- **Locations** Reports the Locations and Domain Names of an IP address.
- **VoIPs** Reports all VoIP/H323 calls through the firewall.

Templates

The following section shows examples of the type of Netflow template tables that are exported. You can perform a Diagnostic Report of your own Netflow Configuration by navigating to INVESTIGATE | Tools | System Diagnostics, and clicking the Download Report button in the Tech Support Report section.
Topics:
- NetFlow Version 5
- NetFlow Version 9
- IPFIX (NetFlow Version 10)
- IPFIX with Extensions

NetFlow Version 5

The NetFlow version 5 datagram consists of a header and one or more flow records, using UDP to send export datagrams. The first field of the header contains the version number of the export datagram. The second field in the header contains the number of records in the datagram, which can be used to search through the records. Because NetFlow version 5 is a fixed datagram, no templates are available, and it follows the format of the tables listed in NetFlow version 5 header format and Netflow version 5 record format.
### NetFlow version 5 header format

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Contents</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-1</td>
<td>version</td>
<td>NetFlow export format version number</td>
</tr>
<tr>
<td>2-3</td>
<td>count</td>
<td>Number of flows exported in this packet (1-30)</td>
</tr>
<tr>
<td>4-7</td>
<td>SysUptime</td>
<td>Current time in milliseconds since the export device booted</td>
</tr>
<tr>
<td>8-11</td>
<td>unix_secs</td>
<td>Current count of seconds since 0000 UTC 1970</td>
</tr>
<tr>
<td>12-15</td>
<td>unix_nsecs</td>
<td>Residual nanoseconds since 0000 UTC 1970</td>
</tr>
<tr>
<td>16-19</td>
<td>flow_sequence</td>
<td>Sequence counter of total flows seen</td>
</tr>
<tr>
<td>20</td>
<td>engine_type</td>
<td>Type of flow-switching engine</td>
</tr>
<tr>
<td>20</td>
<td>engine_id</td>
<td>Slot number of the flow-switching engine</td>
</tr>
<tr>
<td>22-23</td>
<td>sampling_interval</td>
<td>First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval</td>
</tr>
</tbody>
</table>

### Netflow version 5 record format

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Contents</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-3</td>
<td>srcaddr</td>
<td>Source IP address</td>
</tr>
<tr>
<td>4-7</td>
<td>dstaddr</td>
<td>Destination IP address</td>
</tr>
<tr>
<td>8-11</td>
<td>nexthop</td>
<td>IP address of the next hop router</td>
</tr>
<tr>
<td>12-13</td>
<td>input</td>
<td>SNMP index of input interface</td>
</tr>
<tr>
<td>14-15</td>
<td>output</td>
<td>SNMP index of output interface</td>
</tr>
<tr>
<td>10-19</td>
<td>dPkts</td>
<td>Packets in the flow</td>
</tr>
<tr>
<td>20-23</td>
<td>dOctets</td>
<td>Total number of Layer 3 bytes in the packets of the flow</td>
</tr>
<tr>
<td>24-27</td>
<td>First</td>
<td>SysUptime at start of flow</td>
</tr>
<tr>
<td>28-31</td>
<td>Last</td>
<td>SysUptime at the time the last packet of the flow was received</td>
</tr>
<tr>
<td>32-33</td>
<td>srcport</td>
<td>TCP/UDP source port number or equivalent</td>
</tr>
<tr>
<td>34-35</td>
<td>dstport</td>
<td>TCP/UDP destination port number or equivalent</td>
</tr>
<tr>
<td>36</td>
<td>pad1</td>
<td>Unused (zero) bytes</td>
</tr>
<tr>
<td>37</td>
<td>tcp_flags</td>
<td>Cumulative OR of TCP flags</td>
</tr>
<tr>
<td>38</td>
<td>prot</td>
<td>IP protocol type (for example, TCP=6; UDP=17)</td>
</tr>
<tr>
<td>39</td>
<td>tos</td>
<td>IP type of service (ToS)</td>
</tr>
<tr>
<td>40-41</td>
<td>src_as</td>
<td>Autonomous system number of the source, either origin or peer</td>
</tr>
<tr>
<td>42-43</td>
<td>dst_as</td>
<td>Autonomous system number of the destination, either origin or peer</td>
</tr>
<tr>
<td>44</td>
<td>src_mask</td>
<td>Source address prefix mask bits</td>
</tr>
<tr>
<td>45</td>
<td>dst_mask</td>
<td>Destination address prefix mask bits</td>
</tr>
<tr>
<td>46-47</td>
<td>pad2</td>
<td>Unused (zero) bytes</td>
</tr>
</tbody>
</table>
NetFlow Version 9

NetFlow Version 9 Example

<table>
<thead>
<tr>
<th>Netflow-v9 Template ID</th>
<th>Name</th>
<th>Number of Elements</th>
<th>Total Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>Flow</td>
<td>12</td>
<td>41</td>
</tr>
</tbody>
</table>

Field 1, Field bytes = 4
Field 2, Field bytes = 4
Field 4, Field bytes = 1
Field 5, Field bytes = 4
Field 6, Field bytes = 2
Field 7, Field bytes = 2
Field 10, Field bytes = 4
Field 11, Field bytes = 2
Field 12, Field bytes = 4
Field 14, Field bytes = 4
Field 15, Field bytes = 4
Field 21, Field bytes = 4
Field 22, Field bytes = 4

Netflow version 9 template FlowSet fields details the NetFlow version 9 Template FlowSet field descriptions.

**Netflow version 9 template FlowSet fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template ID</td>
<td>The firewall generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the NetFlow template.</td>
</tr>
<tr>
<td>Number of Elements</td>
<td>The amount of fields listed in the NetFlow template.</td>
</tr>
<tr>
<td>Total Length</td>
<td>The total length in bytes of all reported fields in the NetFlow template.</td>
</tr>
<tr>
<td>Field Type</td>
<td>The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.</td>
</tr>
<tr>
<td>Field bytes</td>
<td>The length of the specific Field Type, in bytes.</td>
</tr>
</tbody>
</table>

IPFIX (NetFlow Version 10)

IPFIX (NetFlow version 10) example

<table>
<thead>
<tr>
<th>IPFIX Template ID</th>
<th>Name</th>
<th>Number of Elements</th>
<th>Total Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td>Flow</td>
<td>12</td>
<td>41</td>
</tr>
</tbody>
</table>

Field 1, Field bytes = 4
Field 2, Field bytes = 4
Field 4, Field bytes = 1
Field 5, Field bytes = 4
Field 6, Field bytes = 2
Field 7, Field bytes = 2
Field 10, Field bytes = 4
Field 11, Field bytes = 2
Field 12, Field bytes = 4
Field 14, Field bytes = 4
Field 15, Field bytes = 4
Field 21, Field bytes = 4
Field 22, Field bytes = 4

IPFIX template FlowSet fields describes the IPFIX Template FlowSet Fields.

**IPFIX template FlowSet fields**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template ID</td>
<td>The firewall generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the NetFlow template.</td>
</tr>
<tr>
<td>Number of Elements</td>
<td>The amount of fields listed in the NetFlow template.</td>
</tr>
</tbody>
</table>
### IPFIX template FlowSet fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Length</td>
<td>The total length in bytes of all reported fields in the NetFlow template.</td>
</tr>
<tr>
<td>Field Type</td>
<td>The field type is a numeric value that represents the type of field. Note that values of the field type may be vendor specific.</td>
</tr>
<tr>
<td>Field bytes</td>
<td>The length of the specific Field Type, in bytes.</td>
</tr>
</tbody>
</table>

### IPFIX with Extensions

IPFIX with extensions exports templates that are a combination of NetFlow fields from the aforementioned versions and SonicWall IDs. These flows contain several extensions, such as Enterprise-defined field types and Enterprise IDs.

[NOTE: The SonicWall Specific Enterprise ID (EntID) is defined as 8741.](#)

IPFIX with extensions Name template example is a standard for the IPFIX with extensions templates. The values specified are static and correlate to the Table Name of all the NetFlow exportable templates. Also see IPFIX with extensions template example.

### IPFIX with extensions Name template example

```
<table>
<thead>
<tr>
<th>Table Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TableTemplate id-256, Table Name-Flow IPFIX extn</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-257, Table Name-Table Map</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-258, Table Name-Column Map</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-260, Table Name-user</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-261, Table Name-Application</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-262, Table Name-URL</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-263, Table Name-HTTP</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-264, Table Name-IP</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-265, Table Name-GAV</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-266, Table Name-Anti Spyware</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-267, Table Name-Location Map</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-268, Table Name-Location</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-269, Table Name-Log</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-270, Table Name-wif-stat</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-271, Table Name-core-stat</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-272, Table Name-voip</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-273, Table Name-services</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-274, Table Name-spam</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-275, Table Name-memory</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-276, Table Name-devices</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-277, Table Name-vpn tunnels</td>
<td></td>
</tr>
<tr>
<td>TableTemplate id-278, Table Name-url rating</td>
<td></td>
</tr>
</tbody>
</table>
```
IPFIX with extensions template example

```
IPFIX template ID = 237, Name = Flow IPFIX extn, Number of elements = 39, Total Length = 148

<table>
<thead>
<tr>
<th>Field</th>
<th>Field name</th>
<th>Length</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>2</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>3</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>4</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>5</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>6</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>7</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>8</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>9</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>10</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>11</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>12</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>13</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>14</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>15</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>16</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>17</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>18</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>19</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>20</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>21</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>22</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>23</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>24</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>25</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>26</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>27</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>28</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>29</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>30</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>31</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>32</td>
<td>EncId</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
<tr>
<td>33</td>
<td>Field Bytes</td>
<td>4</td>
<td>uint32</td>
<td>8741</td>
</tr>
</tbody>
</table>
```

SonicWall SonicOS 6.5 Logs and Reporting
Managing Flow Reporting Statistics

41
Connecting to a GMSFlow Server

The **AppFlow Settings > GMS Flow Server** page enables you to establish a connection to a GMSFlow Server.

In the SonicWall Global Management System (GMS), the Flow Server role can be used in a distributed deployment of GMS. In this role, the GMS server runs a single service, which collects SonicWall Flows on the default ports.

The single service that runs in this role is SonicWall Universal Management Suite - Flow Server. The flows are collected and stored in internal databases. To create reports out of these flows, you must have a GMS server in deployment running version 7.1 or higher, and set with the role of Console or All in One. You also need to ensure that these ports are open:

- UDP 2055
- UDP 5055
- TCP 9063
- TCP 9064
- TCP 9065
- TCP 9066
- TCP 9067

The GMS server has a fixed Syslog Facility (Local Use 0), Syslog Format (Default), and Server ID (firewall). Although the Event Profile value for GMS is set to 0 by default, all events are reported to GMS regardless of the profile. GMS is also exempted from Rate Limiting. GMS can be enabled/disabled only in the **Advanced Management** section of the **System Setup | Appliance > Base Settings** page and not in the **Log Settings > Syslog** page.

**Topics:**
- Basic Mode
- Advanced Mode
Basic Mode

Establishing a connection is a two-step process:

1. Establish a connection to the GMSFlow Server.
2. Configure the GMSFlow Server on the Logs & Reporting | AppFlow Settings > Flow Reporting page in SonicOS.

For more detailed information about configuring an AppFlow server with GMS, refer to the latest SonicWall GMS Administration Guide.

To establish a connection to a GMSFlow Server:

1. In GMS, log into the Instant GMSFlow Server.
2. Go to the Network > Settings page.
3. Find and copy the Host IP address of the GMSFlow Server.

On the SonicWall network security appliance:

2. For the Flow Server Configuration Mode, Basic should be selected. (This is the default setting.)
3. In the GMSFlow Server Address field, either:
   - Paste the Host IP address you copied from the GMSFlow Server.
   - Select a predefined address object from the AddrObj dropdown list. You can also create a new address object by choosing Create new address object. For information about creating an address object, see SonicWall SonicOS 6.5 Policies.
4. In the Source IP to use for Collector on a VPN Tunnel field, specify the source IP address for the applicable VPN policy.
   - IMPORTANT: If the GMSFlow server is reachable via a VPN tunnel, then this field must be specified. You can choose an IP from the VPN policy.
5. In the Server Communication Timeout field, enter the number of seconds that the firewall will wait to receive a response from the Flow Server. The range is 60 (default) to 120 seconds.
6. If you want to enable the firewall to send static flows to the Flow Server each time the firewall is rebooted, select the Auto-Synchronize Flow Server option. (This is selected by default.)
7. To test your connection to the GMSFlow Server, click the Test Connectivity button. The connectivity status is displayed.
If you want to manually send static data to the GMSFlow Server, click the **Synchronize Server** button. The synchronicity status is displayed.

**IMPORTANT:** You must click the **Synchronize Server** button once, and once only, after connecting to and registering your SonicWall GMS product.

Click **Accept**.

**Topics:**
- Connecting to a GMSFlow Server
- Advanced Mode

**Advanced Mode**

Advanced Configuration mode allows to specify select more than one GMS Flow server and then set how the flows are directed or balanced between the servers.

Establishing a connection is a two-step process:

1. Establish a connection to the GMSFlow Server.
2. Configure the GMSFlow Server on the **Logs & Reporting | AppFlow Settings > Flow Reporting** page in SonicOS.

For more detailed information about configuring an AppFlow server with GMS, refer to the latest *SonicWall GMS Administration Guide*.

**To establish a connection to a GMSFlow Server:**

1. In GMS, log into the Instant GMSFlow Server.
2. Go to the **Network > Settings** page.
3. Find and copy the Host IP address of the GMSFlow Server.

**On the SonicWall network security appliance:**

1. Navigate to the **Logs & Reporting | AppFlow Settings > GMSFlow Server** page.
2. For the **Flow Server Configuration Mode**, choose **Advanced**.

![Flow Server Configuration Mode](image)

3. Set the **Advanced Flow Server Config Mode**.

![Advanced Flow Server Config Mode](image)

- **ActiveStandby** — If you select this option, flows will be directed first to GMSFlow Server 1 (if available). If GMSFlow Server 1 is not available, flows will be directed to the GMSFlow Server 2 (if available). (This is the default setting.)
• **Load Balancing** — If you select this option, you can choose between these load-balancing configurations:
  
  • **Share-Load** — If both flow servers are available, the flows will be divided equally between the two flow servers.
  
  • **Mirror** — If you select this load-balancing option, all flows will be sent to both flow servers.

4 In the **GMSFlow Server Address** fields, either:
  
  • Paste the Host IP address you copied from the GMSFlow Server.
  
  • Select a predefined address object from the **AddrObj** dropdown list. You can also create a new address object by choosing **Create new address object**. For information about creating an address object, see SonicWall SonicOS 6.5 Policies.

5 In the **Source IP to Use for Collector on a VPN Tunnel** field for each GMSFlow Server, specify the source IP address for the applicable VPN policy.

  🔄 **IMPORTANT**: If the GMSFlow server is reachable via a VPN tunnel, then this field must be specified. You can choose an IP from the VPN policy.

6 In the **Server Communication Timeout** field for each GMSFlow Server, enter the number of seconds that the firewall will wait to receive a response from the Flow Server. The range is 60 (default) to 120 seconds.

7 If you want to enable the firewall to send static flows to a Flow Server each time the firewall is rebooted, select the **Auto-Synchronize Flow Server** option for that GMSFlow Server.

8 To test your connection to a GMSFlow Server, click the **Test Connectivity** button for that GMSFlow Server. The connectivity status is displayed.

9 If you want to manually send static data to a GMSFlow Server, click the **Synchronize Server** button for that GMSFlow Server. The synchronicity status is displayed.

  🔄 **IMPORTANT**: You must click the **Synchronize Server** button once, and once only, after connecting to and registering your SonicWall GMS product.

10 Click **Accept**.

**Topics:**

• Connecting to a GMSFlow Server

• Basic Mode
Logs & Reporting Log Settings

• Configuring Log Settings
• Configuring Syslog Settings
• Configuring Log Automation
• Configuring Name Resolution
• Configuring the Log Analyzer
• Configuring AWS Logs
Configuring Log Settings

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

The Log Settings > Base Setup 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 select storage options, and import and save logging templates.

Topics:

- Table Columns
- Setting Storage Options
- Configuring the Log Severity and Priority
- Top Row Buttons
- Viewing and Filtering the Log
Table Columns

Topics:
- Category Column
- Color Column
- ID Column
- Priority Column
- Gui Column
- Alert Column
- Syslog Column
- Email Column
- Ipfix Column
- Event Count Column
- Edit and Reset Event Count Icons

Category Column

The Category column of the Log Monitor 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 to the left of the category or group name expands or collapses the category or group contents:

<table>
<thead>
<tr>
<th>Category</th>
<th>Color</th>
<th>ID</th>
<th>Priority</th>
<th>Gui</th>
<th>Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td></td>
<td>1220</td>
<td>Inform</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Name Resolution</td>
<td></td>
<td>1221</td>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AppFlow</td>
<td></td>
<td>1222</td>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
<td>1223</td>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td></td>
<td>1224</td>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Request Sent</td>
<td></td>
<td>1225</td>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Update Successful</td>
<td></td>
<td>1226</td>
<td>Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Update Failure</td>
<td></td>
<td>1227</td>
<td>Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Clock Manually Updated</td>
<td></td>
<td>1228</td>
<td>Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td></td>
<td>1229</td>
<td>Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USB Over Current</td>
<td></td>
<td>1230</td>
<td>Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Supply Without Redundancy</td>
<td></td>
<td>1231</td>
<td>Notice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thermal Red Timer Exceeded</td>
<td></td>
<td>1232</td>
<td>Notice</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Color Column

The Color column shows the color with which the event is highlighted in INVESTIGATE | Logs > Event Logs. To change the color of the event, click the Edit icon for the event.

ID Column

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

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

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 affects the Syslog output for the tag "pri=" as well as how the event is treated when performing filtering by priority level. Setting the Event Priority to a level that is lower than the Logging Level causes those events to be filtered out. Also, as GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages must have a minimum Event Priority of Inform.

The Priority column shows the severity or priority of a category, group, or event. For events, a drop-down menu lists the selectable priorities. For categories and groups, the priorities are listed in the dialog when you click 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 indicates whether this item is displayed in INVESTIGATE | Logs > Event Logs. Display of categories and groups is shown with a To show or hide indicator. To change the display for:

- An event, select or deselect the checkbox in the column.
- Categories and groups, click the Edit icon in the column to display the Edit Log Group dialog.
Alert Column
The Alert column shows checkboxes that indicate whether an Alert message is sent for this event, group, or category. Whether the message is sent is shown with a To show or hide indicator. To change whether the Alert message is sent for:

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

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

Event Count Column
The Event Count column shows the count of events by:

- Event level — The number of times that this event has occurred.
- Group level — The total events that occurred within the group.
- Category level — The total events that occurred within the category.
By hovering your mouse over an event count, a pop-up message displays the count of events dropped for these reasons:

- Overflow
- GUI Filter
- Alert Filter
- Syslog Filter
- E-mail Filter
- Priority
- Syslog Event Rate
- Syslog Data Rate

### Edit and Reset Event Count Icons

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

- The **Edit** icon launches the **Edit Log Event**, **Edit Log Group**, or **Edit Log Category** dialog. You can configure all of the attributes for an event, group, or category.

- The **Reset Event Count** icon resets the event counter for an event, a group, or a category, and the event counters of higher levels are recalculated. To reset all counters, use the **Reset Event Count** button above the **Log Settings** table, as described in **Reset Event Count Button**.

### Setting Storage Options

The **Storage** button provides a way to select between the **Built-in Storage** and **Flexible Storage** modules for storing the log files. The Built-in Storage module is used by default if both modules are available on the security appliance. If you change the storage option, SonicOS begins storing log files on the selected storage module immediately. The **Storage** button also provides a way to purge all files from either storage module.

The **Storage** button is disabled if your security appliance does not have any available storage modules.
Unlike Built-in Storage which is meant to be used by only one firewall, the Flexible Storage module is a shared device that can be used on multiple firewalls if successfully activated on each firewall. In the Flexible Storage module, a top-level directory is created with the firewall EPAID as the directory name. Applications create sub-directories inside this top-level directory and store their data there.

**Configuring the Storage Module for Log File Storage**

*To select a storage module:*

1. Navigate to the MANAGE | Logs & Reporting | Log Settings > Base Setup page.
2. Click the Storage button at the top, above the table. The Storage Options dialog displays.

![Storage Options dialog](image)

3. Select Flexible Storage from the Storage Module drop-down list, or leave the default selection of Built-in Storage. Once this setting is saved, this is the storage module to which your log files will be written.
4. Click SAVE.

**Purging a Storage Module**

Purging a storage module removes all the data from it.

*To purge a storage module:*

1. Navigate to the MANAGE | Logs & Reporting | Log Settings > Base Setup page.
2. Click the Storage button at the top, above the table. The Storage Options dialog displays.
3. Select the storage module to purge from the Purge Backups drop-down list.
4 Click the **PURGE NOW** button. A confirmation dialog displays.

5 Click **OK** in the confirmation dialog to confirm the purge.

6 Click **CANCEL** or the X to close the **Storage Options** dialog.

### Configuring the Log Severity and Priority

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

**NOTE:** Alert emails are sent when the **Send Log to E-mail Address** option and the **Send Alerts to E-mail Address** option are configured on the **Log Settings > Automation** page.

**Topics:**
- Setting the Logging Level
- Configuring Event Attributes Globally
- Configuring Event Attributes Selectively

### Setting the Logging Level

The **Logging Level** allows you to filter events by priority. Events with equal or greater priority are passed. Events with a lower priority are dropped. This enables you to filter out lower-level priorities to prevent them being logged in the system.

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

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Inform
To set the logging level:

1. Navigate to the Logs & Reporting | Log Settings > Base Setup page.
2. From the Logging Level drop-down menu, select the logging level you want.

All events with a priority equal to or higher than the selected entry are also logged. For example, if you select Error as the logging level, all messages tagged as Error, as well as all messages with a higher priority such as Critical, Alert, and Emergency, are also displayed. The default value is Debug.

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

Setting the Alert Level

The Alert Level allows you to filter email alerts by alert level. Events with an equal or greater alert level are sent to the specified email address. Events with a lower alert level are ignored. This enables you to filter out lower-level email alerts to reduce the actual emails transmitted.

On the Log Settings > Base Setup page, you can set the baseline alert level to be displayed on the INVESTIGATE | Reports | Log Reports page:

- Emergency
- Alert
- Critical
- Error
- Warning

To set the alert level:

1. Navigate to the Logs & Reporting | Log Settings > Base Setup page.
2. From the Alert Level drop-down menu, select the logging level you want.
All events with a higher alert level than the selected entry are also logged. For example, if you select Error as the logging level, all messages tagged as Error, as well as all messages with a higher alert level, such as Critical, Alert, and Emergency, are also displayed. The default value is Alert.

**TIP:** To display all alert events, select Warning as the alert level.

### Configuring Event Attributes Globally

**NOTE:** For how to configure event attributes selectively, see Configuring Event Attributes Selectively.

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

These global attributes can be modified:

- Event Priority
- Inclusion of events in Log Monitor, Email, and Syslog
- Redundancy filter settings
- Email settings
- Font color when displayed in Log Monitor

**To edit the Category attributes globally:**

1. Navigate to the Logs & Reporting | Log Settings > Base Setup page.
2 Click the Configure icon. The Edit Attributes of All Categories pop-up dialog appears.

![Edit Attributes of All Categories](image)

<table>
<thead>
<tr>
<th>NOTE:</th>
<th>The Enable buttons are solid green ( ) when all categories, groups, and/or events are enabled, white ( ) when all are disabled, and semi-solid ( ) when they are mixed (some enabled, some disabled).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>As this configuration is for all categories, you have to explicitly set the option to “all enabled” by clicking the icon until it is solid green, or to set the option to “all disabled” by clicking the icon until it is white. To configure a single event to be different from the rest of its group or category, you must go into the individual event setting configuration. If you do this, the icon is semi-solid.</td>
</tr>
<tr>
<td></td>
<td>When the fields say Multiple Values, different values have been specified for one or more category, group, or event. To view the individual settings, refer to Configuring Event Attributes Selectively. To change the setting from Multiple Values into one value for all categories, groups, or events while in the Edit Attributes of All Categories dialog, verify that the option was enabled so the field can be accessed for entering the new value. If the option is disabled, the field is dimmed and inaccessible.</td>
</tr>
</tbody>
</table>

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

| 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 GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages must have a minimum Event Priority of Inform. |

| TIP: | The following Redundancy Filter Interval fields enable you to enter time intervals (in seconds) to avoid duplication of a log message within an interval. The range for these intervals is 0 to 86400 seconds. For Syslog messages, the default interval is set to 90 seconds. For alert messages, the default interval is set to 900 seconds. |

| TIP: | The different options are independent of each other, and you can enable any combination of them and set different frequencies of generation for them. For example, you may want an event message emailed to you, but it not shown in the INVESTIGATE | Logs > Event Logs page. These changes will affect the filtering of category- and group-level events that may affect factory-defined events, such as those required by GMS, are ignored. Modifications to specific events (explicit changes), however, may override this built-in protection of GMS-required events. |
4 If you want to display the log events in the Log Monitor, select the Enable icon for the Display Events in Log Monitor option.
   a In the Display Events in Log Monitor Redundancy Filter Interval field, enter the number of seconds that should elapse before allowing the same event to be logged and displayed by the Log Monitor again when that event occurs one after the other. The range is 0 to 86400.

   For example, if you set this value to 60 seconds, then when the event Connection Closed first happens at 1:15 p.m., the next Connection Closed event is not logged until 60 seconds after the first one. Any Connection Closed event occurring within the 60-second interval is dropped.

5 If you want to send events as email alerts, select the Enable icon for the Send Events as E-mail Alerts option.
   a In the Send Events as Email Alerts Redundancy Filter Interval field, enter the number of seconds that should elapse before allowing the same email event to be sent when that email alert occurs one after the other. The range is 0 to 86400.

   For example, if you set this value to 60 seconds, then when an email alert first happens at 1:15 p.m., the next email alert is not sent until 60 seconds after the first one. Any email alert occurring within the 60-second interval is dropped.

6 If you want to report events via Syslog, select the Enable icon for the Report Events via Syslog option.
   a In the Report Events via Syslog Redundancy Filter Interval field, enter the number of seconds that should elapse before allowing the same Syslog messages to be sent when that event occurs one after the other. The range is 0 to 86400.

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

7 To send the Syslogs to a particular Syslog server group, enter the group’s ID in the Use this Syslog Server Profile field. The default is 0. For information about Syslog Server (Event) profiles, see About Event Profiles and Syslog Servers.

8 If you want to report events via IPFIX, select the Enable icon for the Report Events via IPFIX option.
   a In the Report Events via IPFIX Redundancy Filter Interval field, enter the number of seconds that should elapse before allowing the same messages to be sent via IPFIX when events occur one after the other. The range is 0 to 86400.

   For example, if you set this value to 60 seconds, then when a message sent via IPFIX first happens at 1:15 p.m., the next message is not sent until 60 seconds after the first one. Any message occurring within the 60-second interval is dropped.

9 If you want to send the global event log via email, select the Enable icon for the Include Events in Log Digest option.

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

10 If you enabled Include Events in Log Digest, do one of the following for Send Log Digest to Email Address:
   • If you want to use the same email address that is entered in the Log Settings > Automation page even when you change other values in this dialog, select the Leave Unchanged checkbox. This option is enabled by default.
• To change the email address, uncheck the **Leave Unchanged** option and enter a new address in the now-active field.

**TIP:** An email alert is one email sent for each event occurrence as soon as that event has occurred. A Log Digest, on the other hand, is a chronological collation of events sent as a single email in digest format. Because it is a summation of events, the event information time period is a mix of older and newer events.

11 If you want to receive alerts via email based on the global settings in this dialog, do one of the following for **Send Alerts to E-mail Address**:

- If you want to use the same email address that is entered in the Log Settings > Automation page even when you change other values in this dialog, select the **Leave Unchanged** checkbox. This option is enabled by default.
- To change the email address, uncheck the **Leave Unchanged** option and enter a new address in the now-active field.

12 If you want to use a specific color for the global events log, uncheck the **Leave Unchanged** option, which is the default setting. The color selection matrix appears.

![Color Selection Matrix](image)

13 Select the color you want. The **Show Events using Color** square becomes the chosen color.

![Selected Color](image)

14 Click **Accept**.
Configuring Event Attributes Selectively

**NOTE:** For how to configure event attributes globally, see Configuring Event Attributes Globally.

On the Log Settings > Base Setup page, the columns show the main event attributes that can be configured on different levels: category, group, or each event.

![Image](https://example.com/image.png)

**NOTE:** The Edit Log pop-up dialogs may look slightly similar, but the effect of each varies in scope. The:
- *Edit Log Category* dialog modifies settings for all groups that belong to the same category and, consequently, all events in that category.
- *Edit Log Group* dialog modifies settings for all events that belong to that group and, consequently, all events in that group.
- *Edit Log Event* dialog modifies settings for one specific event.

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

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

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

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

Topics:
- Configuring Event Attributes by Category
- Configuring Event Attributes by Group
- Configuring Event Attributes by Event
Configuring Event Attributes by Category

Any changes done at the category level apply to all groups and all events within the selected category.

To set the Event Attributes by category level:
1. In Log Settings > Base Setup, select a specific category.
2. Click the Configure icon to launch the Edit Log Category dialog.
3. Follow the steps in Configuring Event Attributes Globally.

Configuring Event Attributes by Group

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

To set the Event Attributes by group level:
1. In Log Settings > Base Setup, select a specific category.
2. Select a specific group within the category.
3. Click the group’s Configure icon to launch the Edit Log Group dialog.
4. Follow the steps in Configuring Event Attributes Globally.
Configuring Event Attributes by Event

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

To set the Event Attributes by event level:

1. In Log Settings > Base Setup, select a specific category.
2. Select a specific group within the category.
3. Select a specific event within the group.
4. Click the event’s Configure icon to launch the Edit Log Event dialog.

5. Follow the steps in Configuring Event Attributes Globally.

Top Row Buttons

Topics:

- Save Logging Template Button
- Import Logging Template
- Reset Event Count Button
- Cancel Button
- Accept Button
Save Logging Template Button

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

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

Import Logging Template

The Import Template button displays the Import from Log Category Template dialog, which allows you to select and import one of these templates:

- Default Template
- Minimal Template
- Analyzer/Viewpoint/GMS Template

**NOTE:** The Default, Minimal, and Analyzer/Viewpoint/GMS templates are defined at the factory.

Default Template

The Default template restores all log event settings to the SonicWall default values. For each of these log fields:

- Even Priority
- Display Events in Log Monitor
- Send Events as E-mail Alerts
- Report Events via Syslog
- Include Events in Log Digest
- Redundancy Filter Interval
- Send Log Digest to E-mail Address
- Send Alerts E-mail Address
- Show Events using Color
Minimal Template

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

**NOTE:** Only the capture filters are modified; the redundancy filter intervals are left as is.

Analyzer/Viewpoint/GMS Template

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

All configurations are limited to the `Report Events via Syslog` option and its associated `Redundancy Filter Interval`. Events critical to the reporting function of Analyzer, Viewpoint, and GMS will have these fields set to the recommended factory-default values:

- Report Events via Syslog
- Redundancy Filter Interval for Syslog

Firewall Action Template

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

Reset Event Count Button

The Reset Event Count button sets all the event counters to zero (0).

Cancel Button

The Cancel button cancels whatever changes you made and leaves the settings unchanged.

Accept Button

The Accept button applies any changes done in Log Settings > Base Setup page.

Viewing and Filtering the Log

After you have configured logging for your appliance, you can display the INVESTIGATE | Logs > Event Logs quickly by clicking the View Logs icon in the top row.

You can apply, create, and delete custom filters to customize the information you wish to log and view on the INVESTIGATE | Reports > Log Reports page. You can create simple or complex filters, depending on the criteria you specify. By doing so, you can focus on points of interest without distraction from other applications, users, or other traffic data.
You can create filters in these ways:

- Clicking on the Link button on the Log Settings > Base Setup page to display the INVESTIGATE | Logs > Event Logs page and following the procedures described in SonicWall SonicOS 6.5 Investigate.
- Using the Filter View button on the Log Settings > Base Setup page to create a filter at the category, group, or event level.

Topics:

- Adding a Filter
- Viewing a Filter
- Deleting a Filter

Adding a Filter

**NOTE:** The filter is valid only while the Log Settings > Base Setup page is displayed. Displaying another page or logging out deletes the filter.

To create a filter using Filter View:

1. At the top of the Log Settings > Base Setup page, click the Filter Add button next to the Filter View button. The Category Filter Statement pop-up dialog displays.

2. Enter the filter. For example, `priority=warning;id=1221,1222,1149`. You can enter multiple keys separated by a semicolon (;) and for each key, multiple values separated by a comma. A key can be a name (from the Category), priority (from Priority), or ID (from the ID column). Keys are case insensitive.

   **NOTE:** Only one filter is valid at a time. If you add another filter, it replaces the existing one.

3. Click Accept.
The display is changed to reflect the filtered data and a new button, [Filter], appears next to the Filter View button:

![Filter View Button](image)

### Viewing a Filter

For a quick look at the filter, click on the [Filter] button. A small, pop-up window displays the filter under the button.

![Filter View Pop-up](image)

**NOTE:** To close the pop-up, click the triangle or [Filter] on the [Filter] button. Do not click the X in the upper right corner of the pop-up as doing so deletes the filter.

### Deleting a Filter

To delete a filter, click on the X in the Delete Box button in the Filter View button, the [Category Filter] button, or the pop-up dialog. Displaying another page or logging out also deletes the filter.
In addition to displaying event messages in the GUI, the SonicWall security appliance can send the same messages to an external, user-configured Syslog Server for viewing. The Syslog message format can be selected in **Syslog Settings** and the destination Syslog Servers can be specified in the **Syslog Servers** table.

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

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

**NOTE:** See [RCF 3164 - The BSD Syslog Protocol](https://tools.ietf.org/html/rfc3164) for more information.

**NOTE:** Syslog output may be affected by changes to Event Priority for event, group, or global categories made on the **Log Settings > Base Setup** page. For more information, see **Configuring Event Attributes Globally**.

**NOTE:** SonicWall Syslog support requires an external server running a Syslog daemon on a UDP Port. The default port is UDP Port 514, but you can choose a different port.
To display the INVESTIGATE | Logs > Event Logs page, click the Show Log Monitor icon in the upper right corner of the page.

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

Topics:
- About Event Profiles
- About Syslog Server Profiling
- Using a GMS Server for Syslog
- Syslog Settings
- Syslog Servers

**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.

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

The Event Profile is used, along with the Server Name and Port, to uniquely identify a Syslog Server in the Syslog Server table. This allows multiple rows to have same Name, Port combination with different Profiles. Thus, a Syslog Server can be a member of more than one Event Profile group.

**About Syslog Server Profiling**

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

With Syslog Server Profiling, the following new functionality is available:
- Syslog messages can be sent using different settings for different Syslog servers
- There can be multiple groups of Syslog servers
- Different events can be configured to be reported to different groups of Syslog servers

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

Use the Enable checkbox to enable or disable sending of Syslog messages to a specific Syslog server. The settings for Enhanced Syslog and ArcSight format can also be configured individually.
All these settings can be configured from the SonicOS web interface and from the command line interface (CLI). For convenience, the global settings can be used to configure all servers.

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

### Using a GMS Server for Syslog

GMS can be enabled or disabled only on the System > Administration page (for enabling and configuring GMS, see SonicWall SonicOS 6.5 System Setup).

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.

When the firewall is managed using GMS, only the global settings can be configured from GMS. So, if a global setting is changed, it affects all the servers. The settings for an individual server cannot be configured. As GMS 8.1 does not support those tags. When adding a new Syslog Server, therefore, only the hostname and port can be configured; all other fields contain default values.

When GMS is enabled, the GMS 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 GMS server). All other groups can have only 7 servers. The events in the GMS group in the Log Settings > Base Setup page have Profile 0 and cannot be changed. Other events can have a different Profile.

### Syslog Settings

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

**NOTE:** If you are using SonicWall’s Global Management System (GMS) to manage your firewall, the Syslog Format is fixed to Default and the Syslog ID is fixed to firewall. Thus, these fields are greyed-out and can’t be modified. All other fields, however, can still be customized as needed.

**To configure Syslog settings on your firewall:**

1. Navigate to the Logs & Reporting | Log Settings > Syslog page.

![Syslog Settings](image)

2. 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=. Thus, 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.
3 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**

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

1. Default

4 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.
- **WebTrends**
  - WebTrends Syslog format. You must have WebTrends software installed on your system.
- **Enhanced Syslog**
  - Enhanced SonicWall Syslog format.
- **ArcSight**
  - ArcSight Syslog format. The Syslog server must be configured with the ArcSight Logger application to decode the ArcSight messages.

5 If you selected:

- **Default** or **WebTrends**, go to **Step 13**.
- **Enhanced Syslog**, go to **Step 6**.
- **ArcSight**, go to **Step 10**.

6 (Optional) If you selected **Enhanced Syslog**, click the **Enhanced Syslog Fields Settings Configure** icon. The **Enhanced Syslog Settings** pop-up dialog displays.
7 (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.

8 Click Save.

9 Go to Step 13.

10 Optionally, if you selected ArcSight, click the ARCSight CEF Fields Settings Configure icon. ArcSight CEF Fields Settings pop-up dialog displays.

11 Optionally, select the ArcSight options to log. By default, all options are selected; the Host and Event ID options are dimmed as they cannot be changed. To:

- Select all options, click 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.

12 Click Save.

13 Optionally, 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.)
14 Optionally, specify the maximum number of bytes in the Maximum Bytes Per Second field; the minimum is 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.

15 Optionally, select the Enable NDPP Enforcement for Syslog Server.

16 Click Accept.

**Syslog Servers**

<table>
<thead>
<tr>
<th>Event Profile</th>
<th>Server Name</th>
<th>Server Port</th>
<th>Server Facility</th>
<th>Server Format</th>
<th>Server ID</th>
<th>Enable</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 0</td>
<td>0.0.0.0 (V1 IP)</td>
<td>514</td>
<td>Local use 0</td>
<td>Default</td>
<td>firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 0</td>
<td>10.209.26.50 (Default Active VAN IP)</td>
<td>514</td>
<td>Local use 0</td>
<td>Default</td>
<td>firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 0</td>
<td>10.209.28.1 (K1 Default Satbray)</td>
<td>514</td>
<td>Local use 0</td>
<td>Default</td>
<td>firewall</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Event Profile** Profile configured for the Syslog Server.

**Server Name** IP address and name of the Syslog Server.

**Server Port** Port of the Syslog Server.

**Server Facility** Server Facility of the Syslog Server; for a list of Server Facilities, see Syslog Facility.

**Server Format** Format expected by the Syslog Server:
- Default (default)
- WebTrends
- Enhanced Syslog
- ArcSight

**Server ID** ID configured for the Syslog Server; default is firewall.

**Enable** Indicates whether the Syslog Server is enabled and allows you to enable or disable the sending of Syslog messages to a specific Syslog Server.

**Configure** Contains the Edit and Delete icons for a Syslog Server. As a GMS server cannot be deleted or configured through the Log Settings > Syslog 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.
Adding a Syslog Server

To add a Syslog server to the firewall.

1. Go to the Log Settings > Syslog page.
2. Go to the Syslog Servers section.
3. Click Add. The Add Syslog Server dialog appears.
4. Specify the Event Profile for this server in the Event Profile field. The minimum value is 0 (1 group), the maximum is 23 (24 groups), and the default is 0. Each group can have a maximum of 7 Syslog servers.
   
   | NOTE: For GMS, the Event Profile must be 0.

5. Select the Syslog server name or IP address from the Name or IP Address drop-down menu. Messages from the firewall are then sent to the servers.
6. If your Syslog server does not use default port 514, type the port number in the Port Number field.
7. Select the Syslog format from the Syslog Format drop-down menu. The default is Default; for all the options, see Syslog formats.
   
   | NOTE: For GMS, the Syslog format must be Default.

8. 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.
   
   | NOTE: For GMS, the Syslog format must be Local Use 0.
9 Optionally, to limit events logged and thus prevent the internal or external logging mechanism from being overwhelmed by log events, select the **Enable Event Rate Limiting** checkbox.

   **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.

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

   **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.

11 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.

12 Click **OK**.

### Editing a Syslog Server

**To edit a Syslog Server:**

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

![](image)

2 Follow the appropriate Step 4 through Step 12 in **Adding a Syslog Server**.

---

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

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

**IMPORTANT:** You can enable a GMS Syslog Server only on the System > Administration page; see SonicWall SonicOS 6.5 System Setup.

**To enable a single Syslog Server:**
1. Select the checkbox in the Enable column.

**To enable all Syslog Servers:**
1. Click the Enable All button.

Disabling Syslog Servers

**IMPORTANT:** You can disable a GMS Syslog Server only on the System > Administration page; see SonicWall SonicOS 6.5 System Setup.

**To disable a single Syslog Server:**
1. Deselect the checkbox in the Enable column.

**To disable all Syslog Servers:**
1. Click the Disable All button.

Deleting Syslog Servers

**IMPORTANT:** You can delete a GMS Syslog Server only on the System > Administration page; see SonicWall SonicOS 6.5 System Setup.

**To delete a single Syslog Server:**
1. Select the Delete icon in the Configure column.

**To delete all Syslog Servers:**
1. Click the Disable All button.
Configuring Log Automation

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

Topics:
- Email Log Automation
- Health Check E-mail Notification
- Mail Server Settings
- Solera Capture Stack
Email Log Automation

- **Send Log to E-mail address** - 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.

- **Send Alerts to E-mail address** - 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.

- **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.

- **Email Format** - Select whether log emails will 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.
To set up a Health Check E-mail Notification:

1. From the E-mail Schedule drop-down menu, select a pre-defined schedule, Create a new schedule, or Disabled.
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.

Mail Server Settings

The mail server settings allow you to specify the name or IP address of your mail server, the from Email address, and authentication method.

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

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

- **Advanced** - The Advanced button displays the Log Mail Address Setting dialog.

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

To configure your firewall with Solera:

1. Select the Enable Solera Capture Stack Integration option. The options in this section become available.
2. Select the host for the Solera server from the Server drop-down menu. You can dynamically create the host by selecting Create New Host....
3. From the Protocol drop-down menu, select either HTTP or HTTPS. The default is HTTPS.
4. In the Port field, enter the port number for connecting to the Solera server. The default port is 443.
5. In the DeepSee Base URL field, define the format for the base URL for the DeepSee path. The format can include special tokens; in the actual URL, the special tokens are replaced with the actual values. A default format is given.

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
- $sport - 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
- $srcip - source IP address
- $srcport - source port
- $dstip - destination IP address
- $dstport - destination port
6 In the **PCAP Base URL** field, define the format for the base URL for the PCAP path. The format can include special tokens; in the actual URL, the special tokens are replaced with the actual values. For these tokens and their definitions, see **Step 5**. A default format is given.

7 In the **Base64-encoded Link Icon** field, define the Base 64-encoded GIF image to be used as desktop shortcut to the Solera server. Ensure the icon is valid and the size is as small as possible. A default icon is given.

8 From the **Address to link from E-mail Alerts** drop-down menu, select either **Default LAN** (default) or **Default WAN**.
Configuring Name Resolution

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

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

Topics:
- Selecting Name Resolution Settings
- Specifying the DNS Server

Selecting Name Resolution Settings

The firewall appliance can use DNS, NetBIOS, or both to resolve IP addresses and server names.

In the Name Resolution Method list, select:
- None: The security appliance will not attempt to resolve IP addresses and Names in the log reports.
- DNS: The security appliance will use the DNS server you specify to resolve addresses and names.
- NetBIOS: The security appliance will use NetBIOS to resolve addresses and names. If you select NetBIOS, no further configuration is necessary.
- DNS then NetBIOS: The security appliance will first use the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it will try again with NetBIOS.

Specifying the DNS Server

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

1. Select Specify DNS Servers Manually or Inherit DNS Settings Dynamically from WAN Zone. The second choice is selected by default.
2. If you selected to specify a DNS server, enter the IP address for at least one DNS server on your network. You can enter up to three servers.
3. Click Accept in the top left corner of the Log Settings > Name Resolution page to make your changes take effect.
Configuring the Log Analyzer

The Log Settings > Analyzer page enables you to add the IP address and port number of your Analyzer server.

To add an analyzer server connection to your firewall:

1. Navigate to the Logs & Reporting | Log Settings > Analyzer page.
2. Click the Add button. The Add Syslog Server dialog appears.
3. From the Name or IP Address drop-down menu, select the item that you want, or select Create New Address Object.
4. In the Port field, enter the port number for the analyzer.
5. 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.  
WebTrends  WebTrends Syslog format. You must have WebTrends software installed on your system.  
Enhanced Syslog  Enhanced SonicWall Syslog format.  
ArcSight  ArcSight Syslog format. The Syslog server must be configured with the ArcSight Logger application to decode the ArcSight messages.

6 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:

<table>
<thead>
<tr>
<th>Facility</th>
<th>Kernel</th>
<th>User-Level Messages</th>
<th>Mail System</th>
<th>System Daemons</th>
<th>Security/Authorization Messages</th>
<th>Messages Generated Internally by syslogd</th>
<th>Line Printer Subsystem</th>
<th>Network News Subsystem</th>
<th>Clock Daemon (Solaris)</th>
<th>Local Use 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UUCP Subsystem</td>
<td>Clock Daemon (BSP Linux)</td>
<td>AUTHPRV Security/Authorization Messages</td>
<td>FTP Daemon</td>
<td>NTP Subsystem</td>
<td>Log Audit</td>
<td>Log Alert</td>
<td>Local Use 7</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7 In the **Syslog ID** field, the value should be **firewall**.

8 (Optional) To limit events logged and thus prevent the internal or external logging mechanism from being overwhelmed by log events, select the **Enable Event Rate Limiting** checkbox.  

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

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

9 (Optional) To limit events logged and thus prevent the internal or external logging mechanism from being overwhelmed by log events, select the **Enable Data Rate Limiting** checkbox.  

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

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

10 (Optional) To connect to your analyzer through a VPN tunnel, under **Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode**:

   a In the **Local Interface** drop-down menu, choose **Select an interface**.

   b In the **Outbound Interface** drop-down menu, choose **Select a tunnel interface**.

11 Click **OK**.  

   **NOTE:** For information about configuring and managing your Analyzer, refer to the **Analyzer User's Guide**.
The Log Settings > AWS Logs page allows configuration of the Amazon Web Services (AWS) endpoint to which the logs are sent along with settings affecting the frequency with which the data is posted.

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

### Enabling AWS Logs

**NOTE:** In order to send the logs from SonicOS to Amazon CloudWatch Logs, you must first create a Log Group and a Log Stream in AWS.

If you already have an Identity Access Management (IAM) user account with the appropriate permissions to access CloudWatch Logs from the AWS Console:

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

1. Navigate to the MANAGE | Logs & Reporting | Log Settings > AWS Logs page.
2. In the CloudWatch Logs section, select Enable Logging.
3. Select the Region in which you created a Log Group and Log Stream in the AWS Console. (You can change the region used by the firewall either on this page or on the System Setup | Network > AWS Configuration page.)
4. Enter the names of the Log Group and Log Stream that you created in the AWS Console that will hold the logs sent to AWS CloudWatch Logs.
5. The logs will be sent at the specified Synchronization Interval. Change the value of the interval (in seconds) to suit your needs.
6. Optionally, you can click FORCE SYNC to manually synchronize with your AWS Console settings.
7. Click ACCEPT.
Part 3

Logs & Reporting Legal and Support

• Accessing Legal Information
• SonicWall Support
Accessing Legal Information

You can access the SonicWall End User Product Agreement (EUPA) as well as other legal information from the Legal page.

SonicWall End User Product Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT, BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT. YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO HTTPS://WWW.SONICWALL.COM/LEGAL/EUPA for VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT.

The SonicWall End User Product Agreement (the “Agreement”) is made between you, the Customer (“Customer” or “You”) and the Provider, as defined below:

1. Definitions. Capitalized terms not defined in context shall have the meanings assigned to them below:

(a) “Affiliate” means any legal entity controlling, controlled by, or under common control with a party to this Agreement, for so long as such control relationship exists.

(b) “Appliance” means a computer hardware product upon which Software is pre-installed and delivered.

(c) “Documentation” means the user manuals and documentation that Provider makes available for the Products, and all copies of the foregoing.

(d) “Maintenance Services” means Provider’s maintenance and support offering for the Products as identified in the Maintenance Services Section below.

(e) “Partner” means the reseller or distributor that is under contract with Provider or another Partner and is authorized via such contract to resell the Products and/or Maintenance Services.

(f) “Provider” means, (i) for the US, Europe, Middle East, Africa, Latin America, and Taiwan, SonicWall Inc., with its principal place of business located at 4 Polaris Way, Aliso Viejo, CA 92656 USA and (ii) for Asia (other than Taiwan) SonicWall International Ltd, City Gate Park Mahon, Cork, Ireland.

(g) “Products” means the Software and Appliance(s) provided to Customer under this Agreement.

(h) “Software” means the object code version of the software that is delivered on the Appliance and any other software that is later provided to Customer as well as any new versions and releases to such software that are made available to Customer pursuant to this Agreement, and all copies of the foregoing.
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.

SonicOS Logs and Reporting
Updated - June 2018
Software Version - 6.5.2
232-002065-02 Rev A

Copyright © 2018 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 WARRANTIES 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