SonicWall® SonicOS 6.5 Logs and Reporting

Administration

Contents

Part 1. Logs & Reporting | AppFlow Settings

Part 2. Logs & Reporting | Log Settings

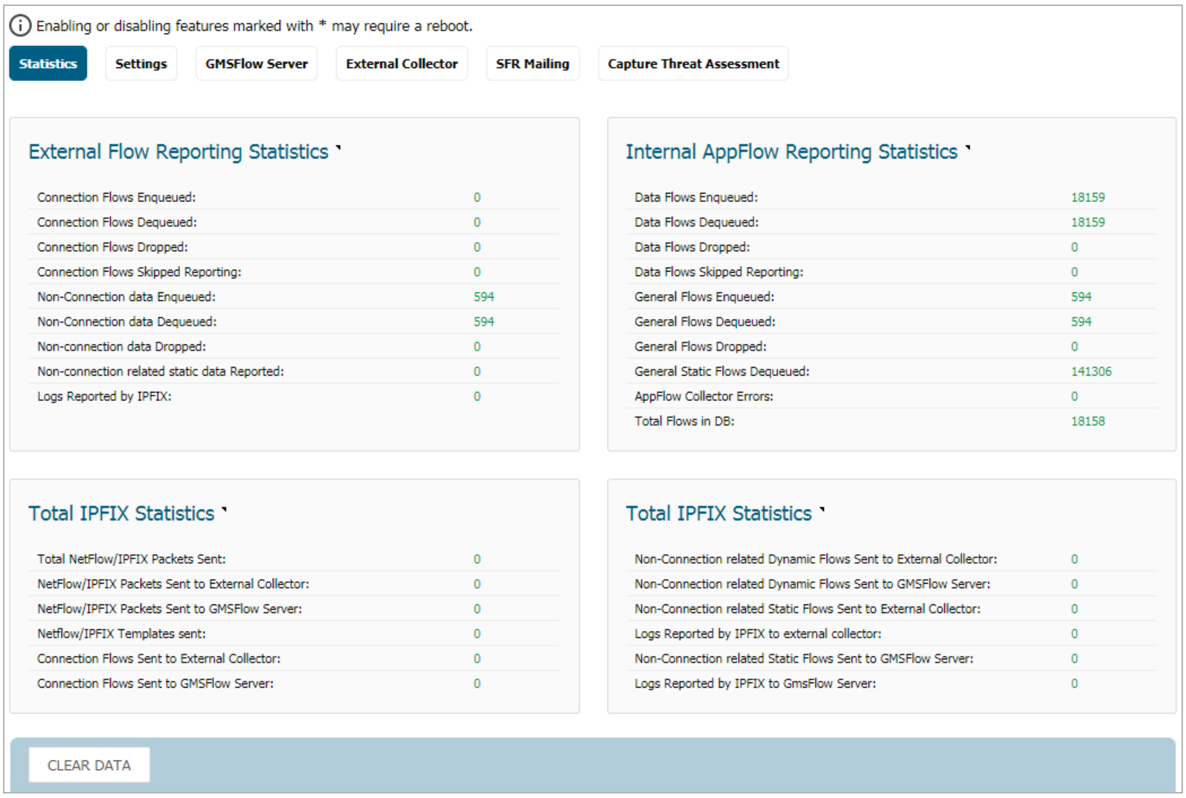
Part 1

Logs & Reporting | AppFlow Settings

1

Managing Flow Reporting Statistics

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



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

External Flow Reporting Statistics

Connection Flows Enqueued:	0
Connection Flows Dequeued:	0
Connection Flows Dropped:	0
Connection Flows Skipped Reporting:	0
Non-Connection data Enqueued:	594
Non-Connection data Dequeued:	594
Non-connection data Dropped:	0
Non-connection related static data Reported:	0
Logs Reported by IPFIX:	0

Internal AppFlow Reporting Statistics

Data Flows Enqueued:	18159
Data Flows Dequeued:	18159
Data Flows Dropped:	0
Data Flows Skipped Reporting:	0
General Flows Enqueued:	594
General Flows Dequeued:	594
General Flows Dropped:	0
General Static Flows Dequeued:	141306
AppFlow Collector Errors:	0
Total Flows in DB:	18158

Total IPFIX Statistics

Total NetFlow/IPFIX Packets Sent:	0
NetFlow/IPFIX Packets Sent to External Collector:	0
NetFlow/IPFIX Packets Sent to GMSFlow Server:	0
Netflow/IPFIX Templates sent:	0
Connection Flows Sent to External Collector:	0
Connection Flows Sent to GMSFlow Server:	0

Total IPFIX Statistics

Non-Connection related Dynamic Flows Sent to External Collector:	0
Non-Connection related Dynamic Flows Sent to GMSFlow Server:	0
Non-Connection related Static Flows Sent to External Collector:	0
Logs Reported by IPFIX to external collector:	0
Non-Connection related Static Flows Sent to GMSFlow Server:	0
Logs Reported by IPFIX to GmsFlow Server:	0

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.

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 **Enable Aggregate AppFlow Report Data Collection** of the **AppFlow Settings > Flow Reporting > Settings** page.

You can clear the AppFlow settings on each page to their default values by clicking **Default Settings** 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 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

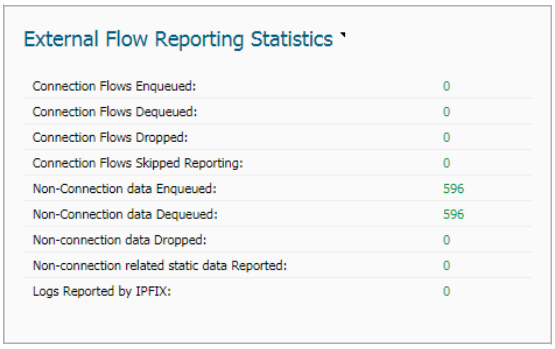
Statistics Screen

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

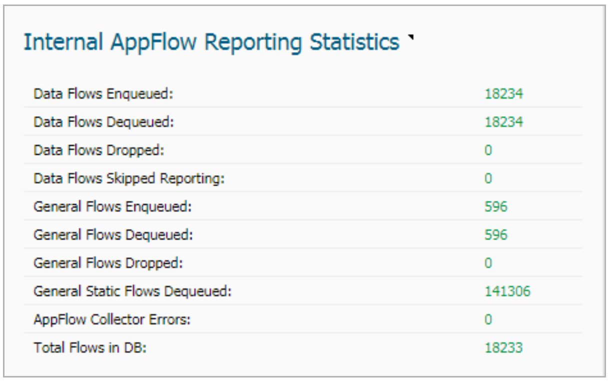


External Flow Reporting Statistics

Connection Flows Enqueued:	0
Connection Flows Dequeued:	0
Connection Flows Dropped:	0
Connection Flows Skipped Reporting:	0
Non-Connection data Enqueued:	596
Non-Connection data Dequeued:	596
Non-connection data Dropped:	0
Non-connection related static data Reported:	0
Logs Reported by IPFIX:	0

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 because of 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



Internal AppFlow Reporting Statistics

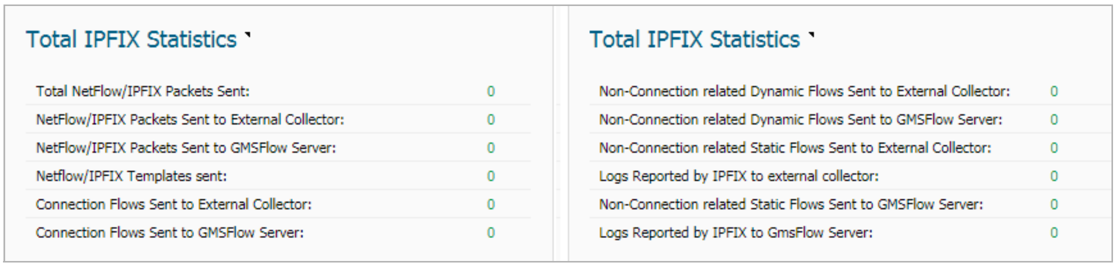
Data Flows Enqueued:	18234
Data Flows Dequeued:	18234
Data Flows Dropped:	0
Data Flows Skipped Reporting:	0
General Flows Enqueued:	596
General Flows Dequeued:	596
General Flows Dropped:	0
General Static Flows Dequeued:	141306
AppFlow Collector Errors:	0
Total Flows in DB:	18233

This statistic	Displays the total number of
Data Flows Enqueued:	Connection-related flows that have been queued to the AppFlow collector.
Data Flows Dequeued:	All connection-related flows that have been successfully inserted into the database.
Data Flows Dropped:	Connection-related flows that failed to get inserted into the database because of a high connection rate.
Data Flows Skipped Reporting:	Connection-related flows that skipped reporting.
General Flows Enqueued:	All non-connection-related flows in the database queue.
General Flows Dequeued:	All non-connection-related flows successfully inserted into the database.
General Flows Dropped:	All non-connection-related flows that failed to be inserted into the database because of a high rate (too many requests).

This statistic	Displays the total number of
General Static Flows Dequeued:	All non-connection-related static flows successfully inserted into the database.
AppFlow Collector Errors:	AppFlow database errors.
Total Flows in DB:	Connection-related flows in the database.

Total IPFIX Statistics

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



Total IPFIX Statistics

Total NetFlow/IPFIX Packets Sent:	0
NetFlow/IPFIX Packets Sent to External Collector:	0
NetFlow/IPFIX Packets Sent to GMSFlow Server:	0
Netflow/IPFIX Templates sent:	0
Connection Flows Sent to External Collector:	0
Connection Flows Sent to GMSFlow Server:	0

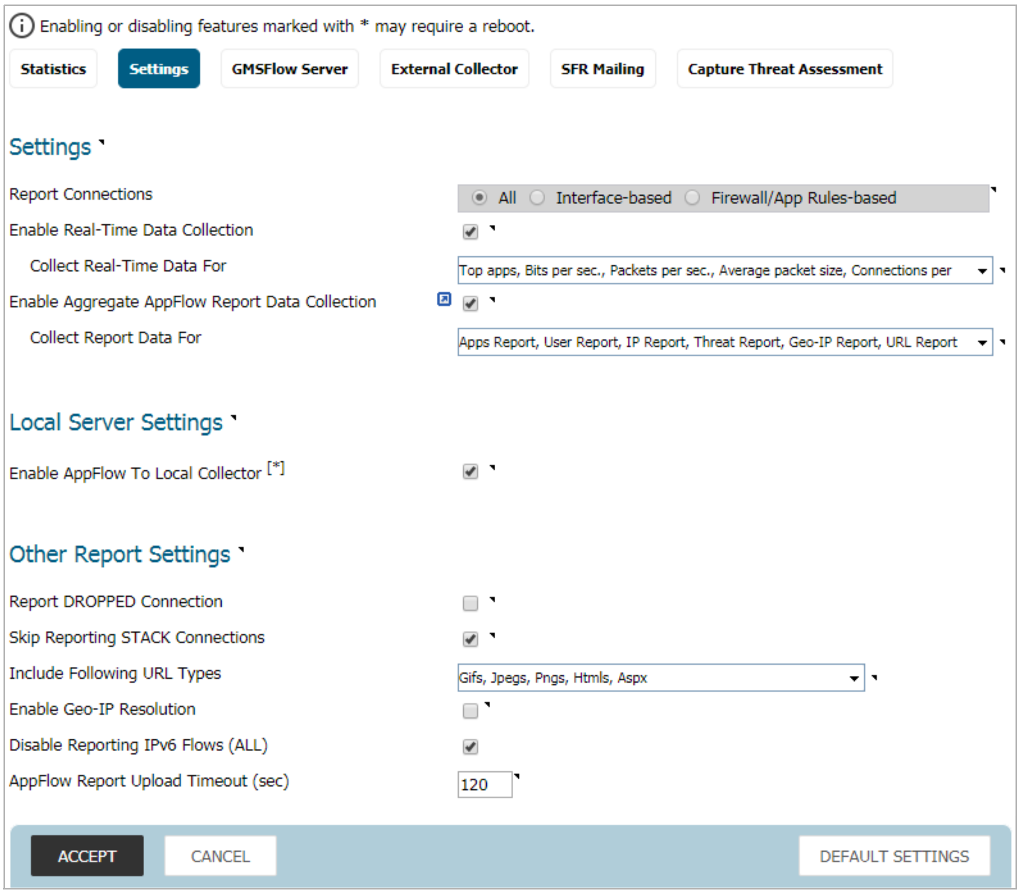
Total IPFIX Statistics

Non-Connection related Dynamic Flows Sent to External Collector:	0
Non-Connection related Dynamic Flows Sent to GMSFlow Server:	0
Non-Connection related Static Flows Sent to External Collector:	0
Logs Reported by IPFIX to external collector:	0
Non-Connection related Static Flows Sent to GMSFlow Server:	0
Logs Reported by IPFIX to GmsFlow Server:	0

This statistic	Displays the total number of
Total NetFlow/IPFIX Packets Sent:	IPFIX/NetFlow packets sent to the all/external collector/AppFlow server/GMSFlow server collected so far.
NetFlow/IPFIX Packets Sent to External Collection:	IPFIX/NetFlow packets sent to the external collector so far.
Netflow/IPFIX Packets Sent to GMSFlow Server	IPFIX/NetFlow packets sent to the GMSFlow collector so far.
NetFlow/IPFIX Templates Sent	IPFIX/NetFlow templates sent to the all/external collector/AppFlow server/GMSFlow serve.
Connection Flows Sent to External Collector	Connection/static/general flows that have been reported to the, external collector.
Connection Flows Sent to GMSFlow Server	Connection/static/general flows that have been reported to the r GMSFlow server.
Non-Connection related Dynamic Flows Sent to External Collector:	IPFIX/NetFlow packets sent to the external collector so far.
Non-Connection related Dynamic Flows Sent to GMSFlow Server:	IPFIX/NetFlow packets sent to the GMSFlow server so far.
Non-Connection related Static Flows Sent to External Collector:	Connection/static/general flows that have been reported to the AppFlow collector or external collector.
Logs Reported by IPFIX to external collector	Logs reported to the external collector by IPFIX so far.
Non-Connection related Static Flows Sent to GMSFlow Server:	Connection/static/general flows that have been reported to the GMSFlow server.
Logs Reported by IPFIX to **GMSFlow Server**	Logs reported to the GMSFlow server by IPFIX so far.

Settings Screen

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



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

Settings

Report Connections: ● All ○ Interface-based ○ Firewall/App Rules-based

Enable Real-Time Data Collection ☑

Collect Real-Time Data For: Top apps, Bits per sec., Packets per sec., Average packet size, Connections per

Enable Aggregate AppFlow Report Data Collection ☑

Collect Report Data For: Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL Report

Local Server Settings

Enable AppFlow To Local Collector [*] ☑

Other Report Settings

Report DROPPED Connection □

Skip Reporting STACK Connections ☑

Include Following URL Types: Gifs, Jpegs, Pngs, Htmls, Aspx

Enable Geo-IP Resolution □

Disable Reporting IPv6 Flows (ALL) ☑

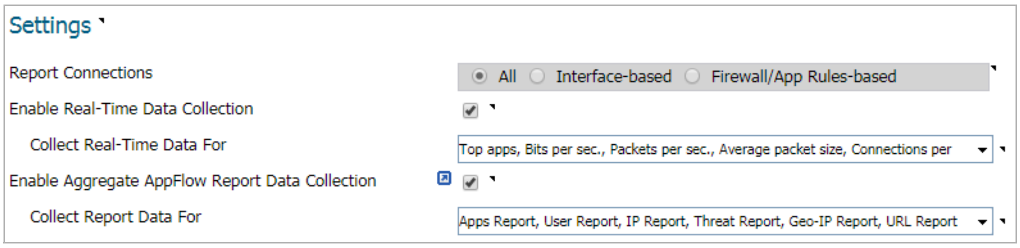
AppFlow Report Upload Timeout (sec): 120

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.



Settings

Report Connections: ● All ○ Interface-based ○ Firewall/App Rules-based

Enable Real-Time Data Collection ☑

Collect Real-Time Data For: Top apps, Bits per sec., Packets per sec., Average packet size, Connections per

Enable Aggregate AppFlow Report Data Collection ☑

Collect Report Data For: Apps Report, User Report, IP Report, Threat Report, Geo-IP Report, URL Report

- **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.	**Multicore Monitor**
Memory util.	**Memory Usage**

- **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.

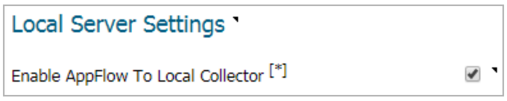
  When this setting is disabled, the AppFlow Reports does not collect or display data.

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

- **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.



Local Server Settings

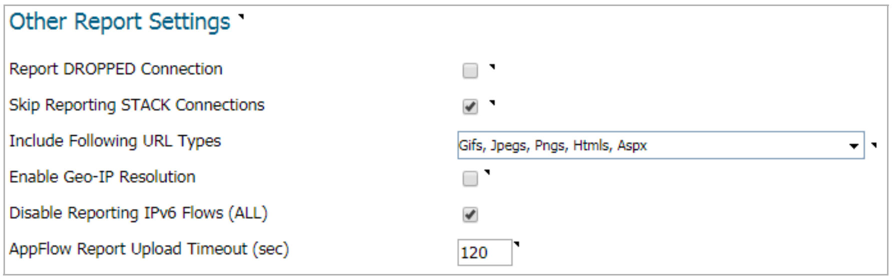
Enable AppFlow To Local Collector [*] ☑

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 might 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.



Other Report Settings

Report DROPPED Connection	□
Skip Reporting STACK Connections	☑
Include Following URL Types	Gifs, Jpegs, Pngs, Htmls, Aspx
Enable Geo-IP Resolution	□
Disable Reporting IPv6 Flows (ALL)	☑
AppFlow Report Upload Timeout (sec)	120

- **Report DROPPED Connection**—If enabled, connections that are dropped because of firewall rules are not reported. This option is enabled by default.
- **Skip Reporting STACK Connections**—If enabled, the firewall does 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)

  Jsons

  Css

  Htmls (selected by default)

Js

Xmls

Aspx (selected by default)

Cms

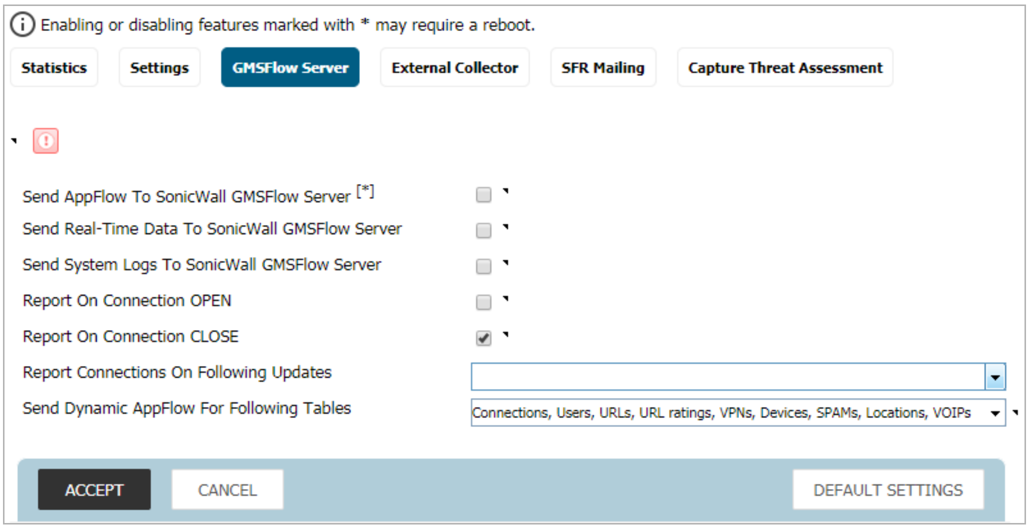
- **Enable Geo-IP Resolution**—Enables Geo-IP resolution. If disabled, the AppFlow Monitor does not group flows based on country under **Initiators** and **Responders** tabs. This setting is unchecked (disabled) by default.

  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.



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

Send AppFlow To SonicWall GMSFlow Server [*] □

Send Real-Time Data To SonicWall GMSFlow Server □

Send System Logs To SonicWall GMSFlow Server □

Report On Connection OPEN □

Report On Connection CLOSE ☑

Report Connections On Following Updates

Send Dynamic AppFlow For Following Tables: Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs

- **Send AppFlow to SonicWall GMSFlow Server** – The SonicWall appliance sends AppFlow data through 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 through redirection of another SonicWall appliance.

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

- **Send Real-Time Data to SonicWall GMSFlow Server** – The SonicWall appliance sends real-time data through 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 through redirection on a SonicWall appliance.

- **Send System Logs to SonicWall GMSFlow Server** – The SonicWall firewall sends system logs through 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 might 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

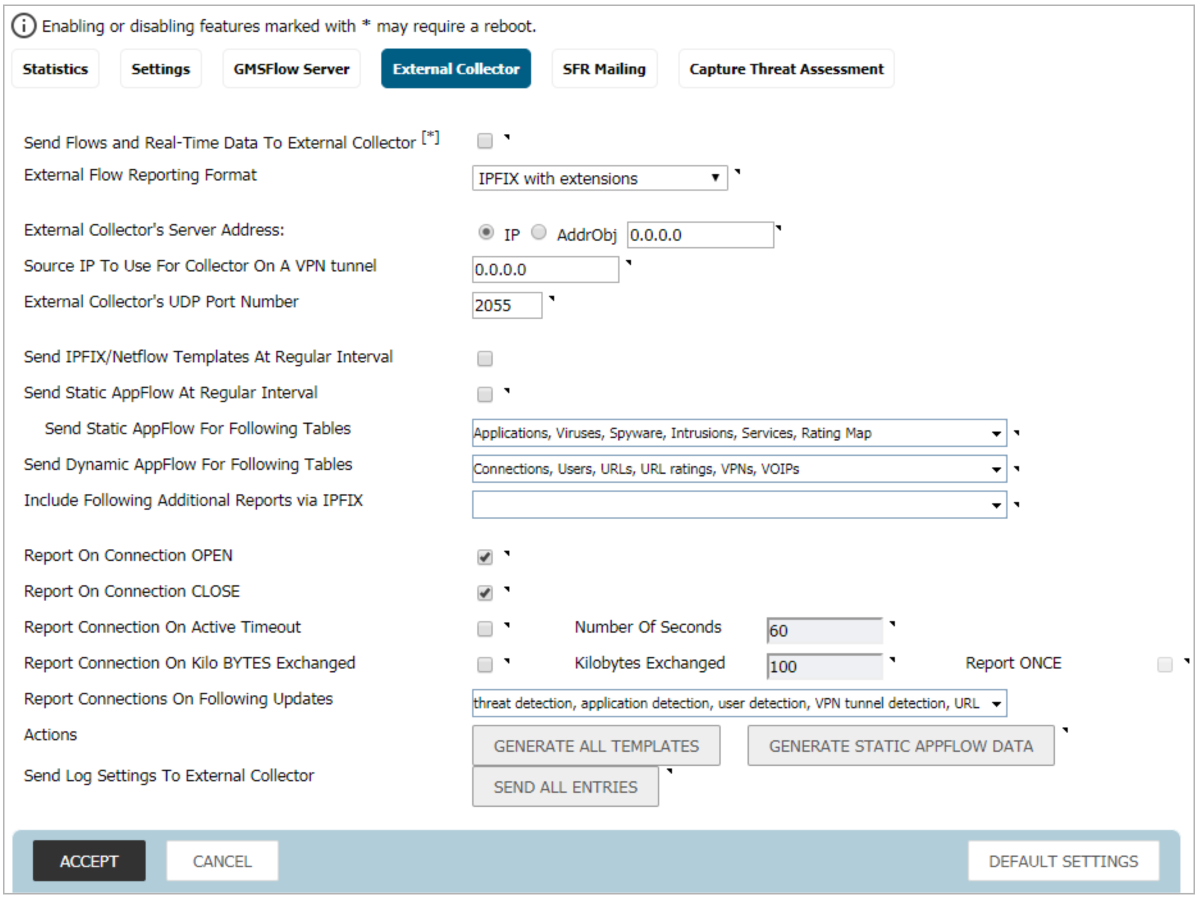
  Locations

  VOIPs

  IMPORTANT: In IPFIX with extension mode, the firewall can generate reports for selected tables. As the firewall does not cache this data, some of the flows not sent could create failures 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.



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

Send Flows and Real-Time Data To External Collector [*] □

External Flow Reporting Format: IPFIX with extensions

External Collector's Server Address: ● IP ○ AddrObj 0.0.0.0

Source IP To Use For Collector On A VPN tunnel: 0.0.0.0

External Collector's UDP Port Number: 2055

Send IPFIX/Netflow Templates At Regular Interval □

Send Static AppFlow At Regular Interval □

Send Static AppFlow For Following Tables: Applications, Viruses, Spyware, Intrusions, Services, Rating Map

Send Dynamic AppFlow For Following Tables: Connections, Users, URLs, URL ratings, VPNs, VOIPs

Include Following Additional Reports via IPFIX:

Report On Connection OPEN ☑

Report On Connection CLOSE ☑

Report Connection On Active Timeout □ Number Of Seconds 60

Report Connection On Kilo BYTES Exchanged □ Kilobytes Exchanged 100 Report ONCE □

Report Connections On Following Updates: threat detection, application detection, user detection, VPN tunnel detection, URL

Actions

Send Log Settings To External 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 might 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)	**IPFIX**
NetFlow version-9	**IPFIX with extensions** [1]

  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 that 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:

    connections
    URLs
    devices
    threats (viruses/spyware/intrusion)
    users
    logs
    SPAMs
    applications
    devices
    wireless
    real-time health (memory/CPU/face statistics)
    locations
    VPN tunnels

    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 through Netflow/IPFIX. This IP address must be reachable from the SonicWall firewall for the collector to generate flow reports. If the collector is reachable through 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)
    Viruses (selected by default)
    Spyware (selected by default)
    Intrusions (selected by default)
    Location Map
    Services (selected by default)
    Rating Map (selected by default)
    Table Map
    Column 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 does not cache this information, some of the flows not sent could create failures when correlating flows with other related data.

  Connections (selected by default)

  Users (selected by default)

  URLs (selected by default)

  URL ratings (selected by default)

  VPNs (selected by default)

  Devices

  SPAMs

  Locations

  VoIPs (selected by default)

- **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 five seconds.

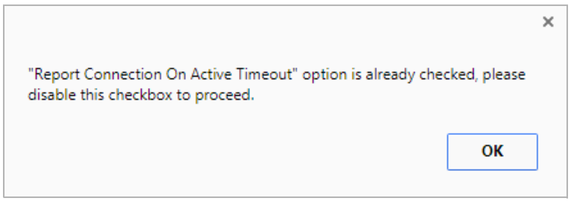
  NOTE: This option is available with **IPFIX with extensions** only.

  - **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.

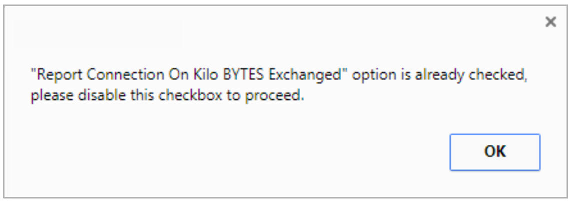
- **Report On Connection OPEN**—Reports flows when a new connection is established. All associated data related to that connection might not be available when the connection is opened. This option, however, enables flows to show up on the external collector as soon as the new connection is established. 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**:
>
> 
>
> "Report Connection On Active Timeout" option is already checked, please disable this checkbox to proceed.
>
>

  - **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**:
>
> 
>
> "Report Connection On Kilo BYTES Exchanged" option is already checked, please disable this checkbox to proceed.
>
>

  - **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 drop-down menu to enable connection reporting for the following (by default, all are selected):

This selection	Reports flows
threat detection	Specific to threats. Upon detections of virus, intrusion, or spyware, the flow is reported again.
application detection	Specific to applications. Upon completing 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.
user detection	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.
VPN tunnel detection	Sent through the VPN tunnel. When flows sent over the VPN tunnel are identified, the flow is reported again.

- **Actions**—Generate templates and static flow data asynchronously when you click these buttons:
  - **Generate ALL Templates** — Click 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 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 **Send All Entries**.

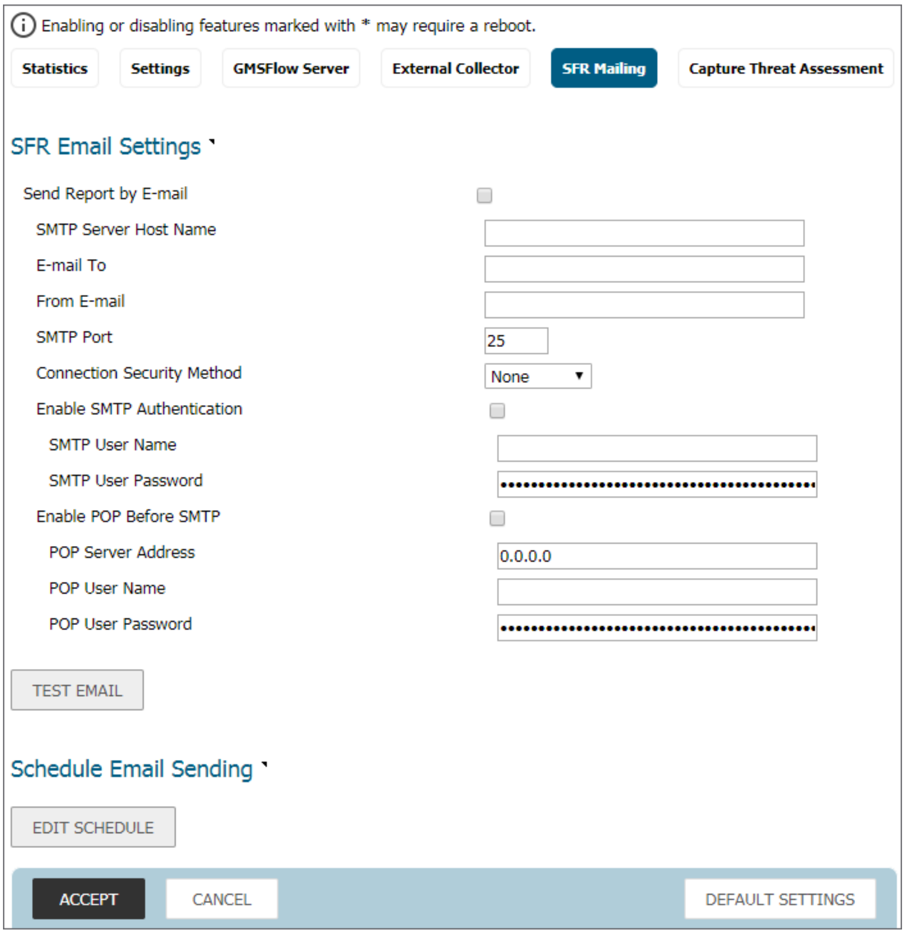
  ⓘ **TIP:** This option displays only when **IPFIX with extensions** is selected for **External Flow Reporting Format**.

  ⓘ **NOTE:** Ensure the connection between SonicOS and the external collector server is ready before clicking **Send All Entries**.

  ⓘ **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 might have been edited.

SFR Mailing Screen

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



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

SFR Email Settings

Send Report by E-mail	□
SMTP Server Host Name	
E-mail To	
From E-mail	
SMTP Port	25
Connection Security Method	None
Enable SMTP Authentication	□
SMTP User Name	
SMTP User Password	••
Enable POP Before SMTP	□
POP Server Address	0.0.0.0
POP User Name	
POP User Password	••

Schedule Email Sending

Topics:

- SFR Email Settings
- Scheduling SFR Reports by Email

SFR Email Settings

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

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

2 Click the **SFR Mailing** tab.

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

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 **Enable SMTP Authentication** 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 **POP Before SMTP** 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.

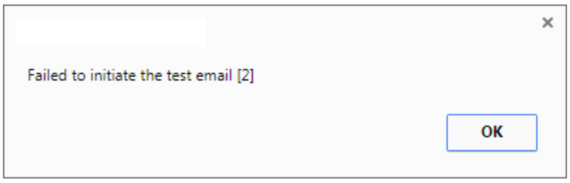
7 Click **Accept**.

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 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:

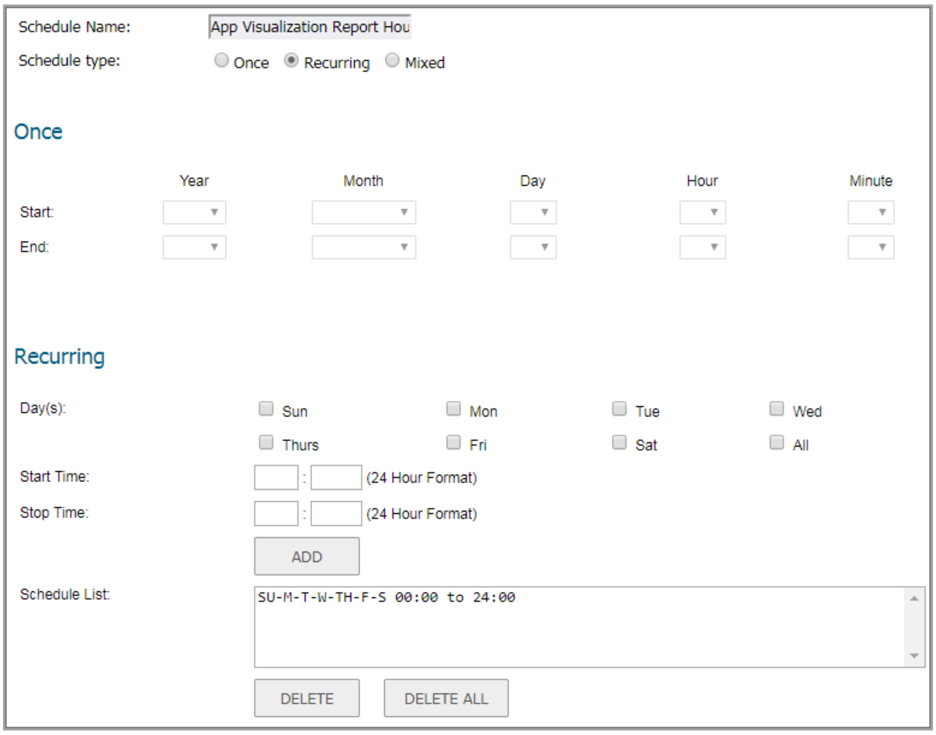
1 Navigate to **MANAGE | Logs & Report > Appflow Settings > Flow Reporting**.

2 Click the **SFR Mailing** tab.

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

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

5 The **Add Schedule** dialog box appears:



Schedule Name: App Visualization Report Hou

Schedule type: ○ Once ● Recurring ○ Mixed

Schedule List: SU-M-T-W-TH-F-S 00:00 to 24:00

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.

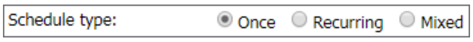
Topics:

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

Scheduling One-Time Delivery of the SFR

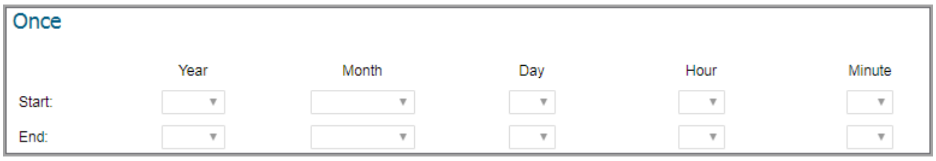
To schedule one-time delivery of the SonicFlow Report (SFR):

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



Schedule type: ● Once ○ Recurring ○ Mixed

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.

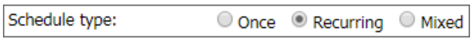


3 Click **OK**.

Scheduling Recurring Delivery of the SFR

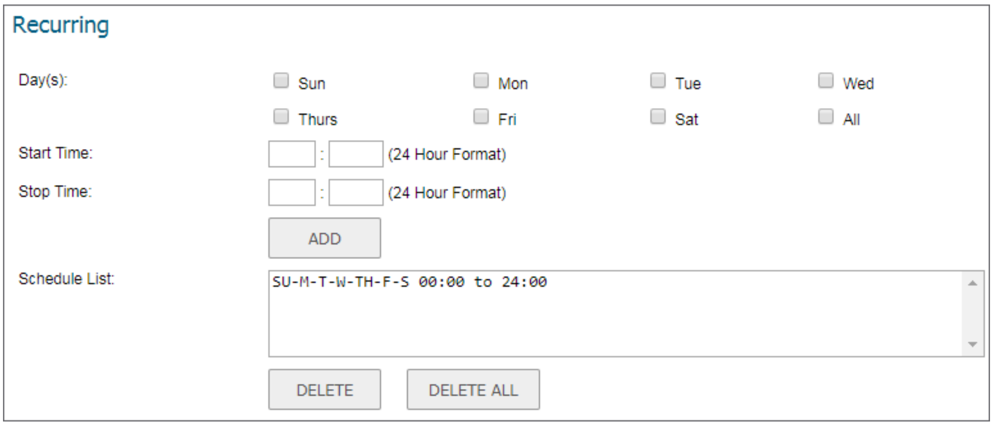
To schedule recurring delivery of the SonicFlow Report (SFR):

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



Schedule type: ○ Once ● Recurring ○ Mixed

2. In the **Recurring** section:



Recurring

Day(s): □ Sun □ Mon □ Tue □ Wed □ Thurs □ Fri □ Sat □ All

Start Time: ___ : ___ (24 Hour Format)

Stop Time: ___ : ___ (24 Hour Format)

Schedule List:

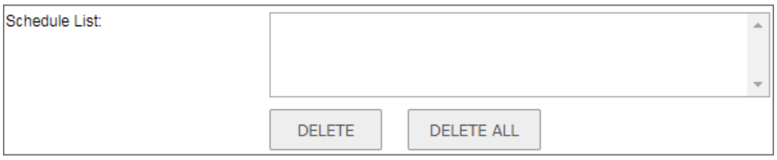
```
SU-M-T-W-TH-F-S 00:00 to 24:00
```

   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.



Schedule List:

To delete selected scheduled reports:

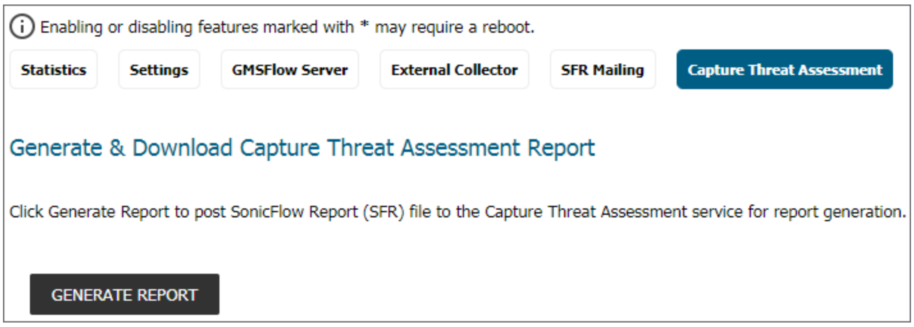
1. Select the reports to be deleted in the **Schedule List**.
2. Click **Delete**. The reports you selected are deleted from the list.
3. Click **OK**.

To delete all scheduled reports:

1. Click **Delete All**. All of the reports are 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.



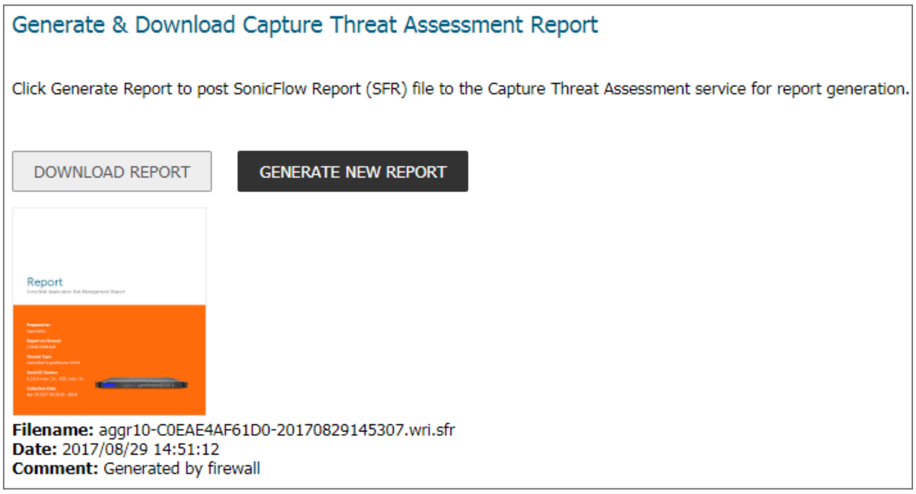
ⓘ Enabling or disabling features marked with * may require a reboot.

Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

To generate and post the SonicFlow Report (SFR):

1. Navigate to the **Capture Threat Assessment** screen on the **Logs & Reporting | AppFlow Settings > Flow Reporting** page.
2. Click **Generate Report**.
3. After the report is generated, you have the option to download the report or generate a new one.



Generate & Download Capture Threat Assessment Report

Click Generate Report to post SonicFlow Report (SFR) file to the Capture Threat Assessment service for report generation.

Filename: aggr10-C0EAE4AF61D0-20170829145307.wri.sfr
Date: 2017/08/29 14:51:12
Comment: Generated by firewall

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 that 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 might only require originating and terminating router flow information whereas monitoring applications might 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 that 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 that 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

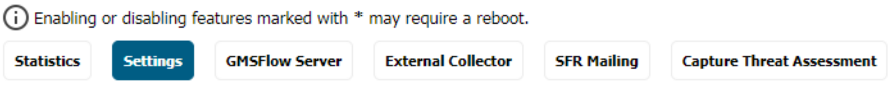
Depending on the type of flows you are collecting, you need to determine which type of reporting works best with your setup and configuration. This section includes configuration examples for each supported NetFlow solution, as well as configuring a second appliance to act as a collector.

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

Configuring NetFlow Version 5

To configure Netflow version 5 flow reporting:

1 Click **Settings**.


Enabling or disabling features marked with * may require a reboot.
Statistics
Settings
GMSFlow Server
External Collector
SFR Mailing
Capture Threat Assessment

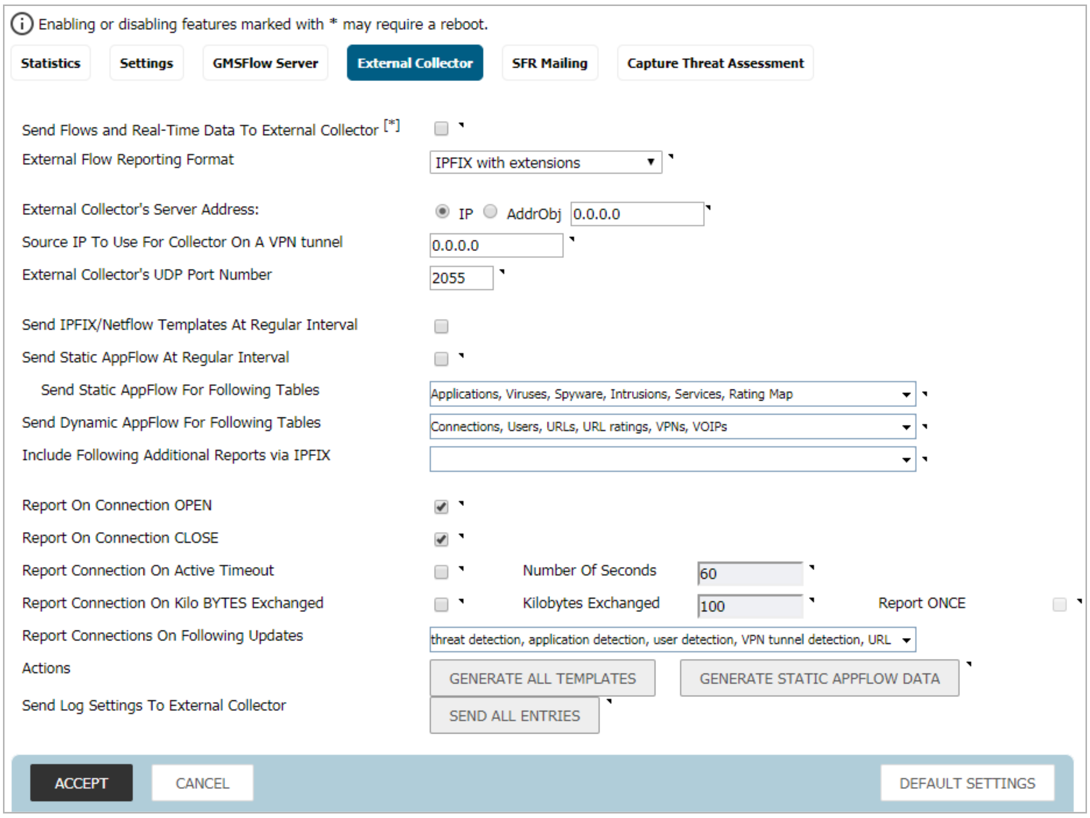
2 For **Report Connections** in the **Settings** section, select one of these radio buttons:

- **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.



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

Send Flows and Real-Time Data To External Collector [*] □

External Flow Reporting Format: IPFIX with extensions

External Collector's Server Address: ● IP ○ AddrObj 0.0.0.0

Source IP To Use For Collector On A VPN tunnel: 0.0.0.0

External Collector's UDP Port Number: 2055

Send IPFIX/Netflow Templates At Regular Interval □

Send Static AppFlow At Regular Interval □

Send Static AppFlow For Following Tables: Applications, Viruses, Spyware, Intrusions, Services, Rating Map

Send Dynamic AppFlow For Following Tables: Connections, Users, URLs, URL ratings, VPNs, VOIPs

Include Following Additional Reports via IPFIX:

Report On Connection OPEN ☑

Report On Connection CLOSE ☑

Report Connection On Active Timeout □ Number Of Seconds 60

Report Connection On Kilo BYTES Exchanged □ Kilobytes Exchanged 100 Report ONCE □

Report Connections On Following Updates: threat detection, application detection, user detection, VPN tunnel detection, URL

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

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**.

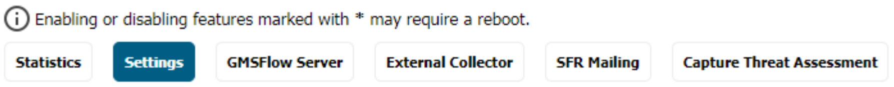
9 Click **Accept** at the top of the page.

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

Configuring NetFlow Version 9

To configure Netflow version 9 flow reporting:

1 Click **Settings**.



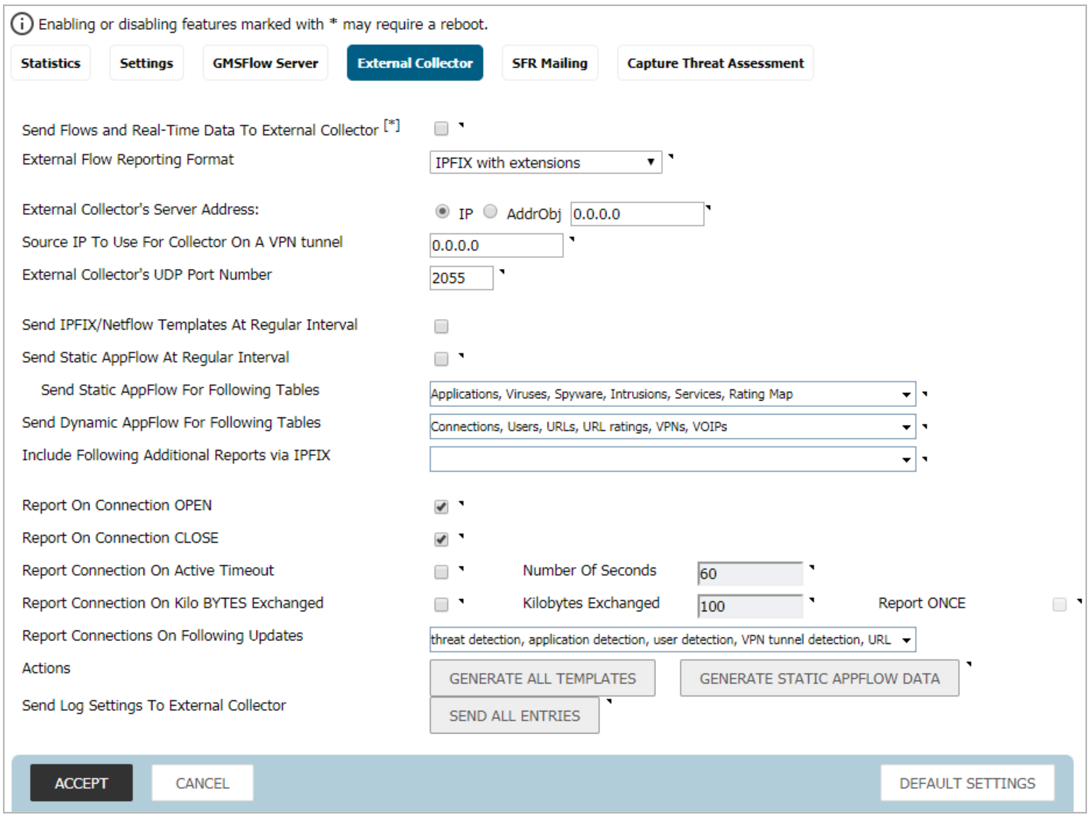
ⓘ Enabling or disabling features marked with * may require a reboot.

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**.



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

Send Flows and Real-Time Data To External Collector [*]	□
External Flow Reporting Format	IPFIX with extensions
External Collector's Server Address:	● IP ○ AddrObj 0.0.0.0
Source IP To Use For Collector On A VPN tunnel	0.0.0.0
External Collector's UDP Port Number	2055
Send IPFIX/Netflow Templates At Regular Interval	□
Send Static AppFlow At Regular Interval	□
Send Static AppFlow For Following Tables	Applications, Viruses, Spyware, Intrusions, Services, Rating Map
Send Dynamic AppFlow For Following Tables	Connections, Users, URLs, URL ratings, VPNs, VOIPs
Include Following Additional Reports via IPFIX	
Report On Connection OPEN	☑
Report On Connection CLOSE	☑
Report Connection On Active Timeout	□ Number Of Seconds 60
Report Connection On Kilo BYTES Exchanged	□ Kilobytes Exchanged 100 Report ONCE □
Report Connections On Following Updates	threat detection, application detection, user detection, VPN tunnel detection, URL
Actions	GENERATE ALL TEMPLATES GENERATE STATIC APPFLOW DATA
Send Log Settings To External Collector	SEND ALL ENTRIES

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

> ⓘ **IMPORTANT:** When enabling this option, you might 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.

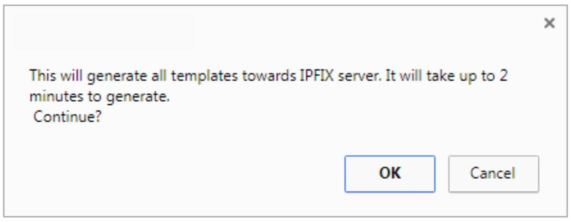
7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

> ⓘ **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 **Generate ALL Templates** to begin generating templates. A message requesting confirmation displays.

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



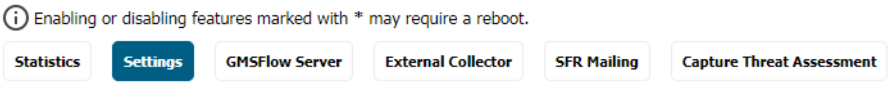
This will generate all templates towards IPFIX server. It will take up to 2 minutes to generate.
Continue?

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**.



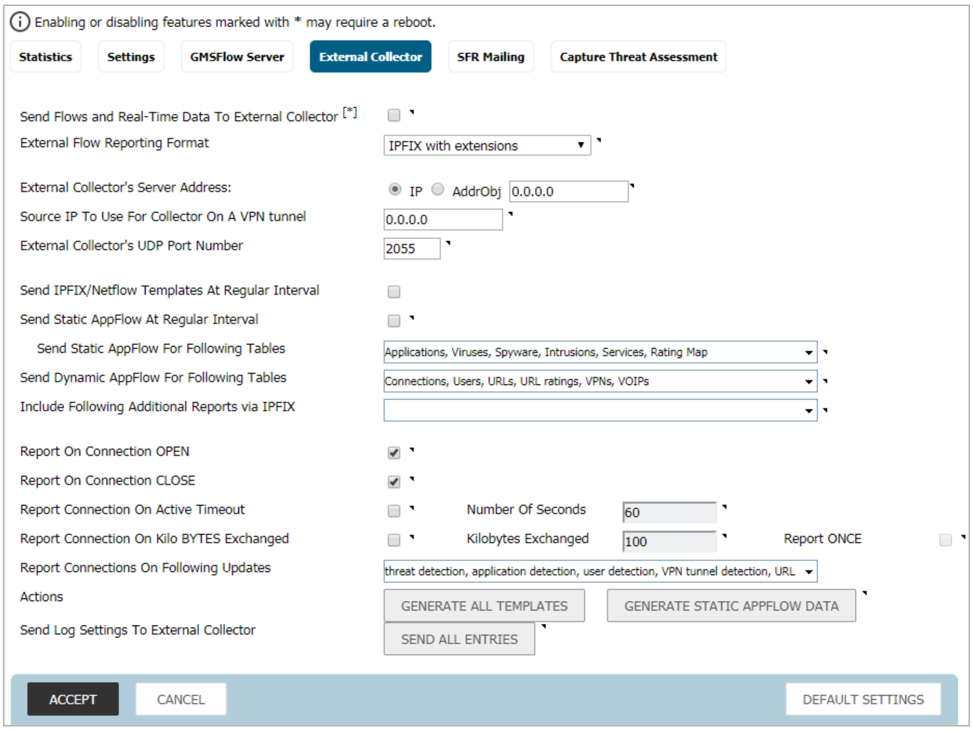
ⓘ Enabling or disabling features marked with * may require a reboot.

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**.



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

Send Flows and Real-Time Data To External Collector [*]	□
External Flow Reporting Format	IPFIX with extensions
External Collector's Server Address:	● IP ○ AddrObj 0.0.0.0
Source IP To Use For Collector On A VPN tunnel	0.0.0.0
External Collector's UDP Port Number	2055
Send IPFIX/Netflow Templates At Regular Interval	□
Send Static AppFlow At Regular Interval	□
Send Static AppFlow For Following Tables	Applications, Viruses, Spyware, Intrusions, Services, Rating Map
Send Dynamic AppFlow For Following Tables	Connections, Users, URLs, URL ratings, VPNs, VOIPs
Include Following Additional Reports via IPFIX	
Report On Connection OPEN	☑
Report On Connection CLOSE	☑
Report Connection On Active Timeout	□ Number Of Seconds 60
Report Connection On Kilo BYTES Exchanged	□ Kilobytes Exchanged 100 Report ONCE □
Report Connections On Following Updates	threat detection, application detection, user detection, VPN tunnel detection, URL
Actions	GENERATE ALL TEMPLATES GENERATE STATIC APPFLOW DATA
Send Log Settings To External Collector	SEND ALL ENTRIES

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

> **IMPORTANT:** When enabling this option, you might 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.

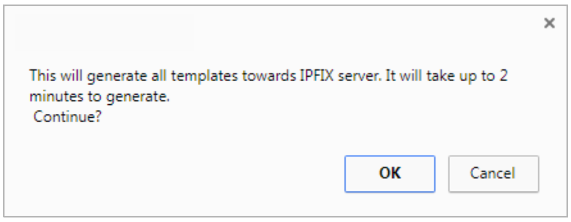
7 Optionally, for the **Source IP to Use for Collector on a VPN Tunnel**, specify the source IP if the external collector must be reached by a VPN tunnel.

> **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 **Generate ALL Templates** to begin generating templates. A message requesting confirmation displays.

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



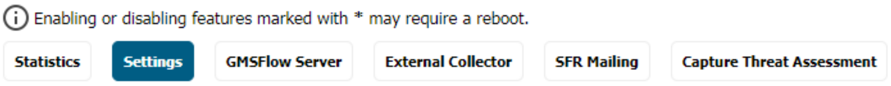
This will generate all templates towards IPFIX server. It will take up to 2 minutes to generate.
Continue?

10 After the templates have been generated, click **Accept**.

Configuring IPFIX with Extensions

To configure IPFIX with extensions flow reporting:

1 Click **Settings**.



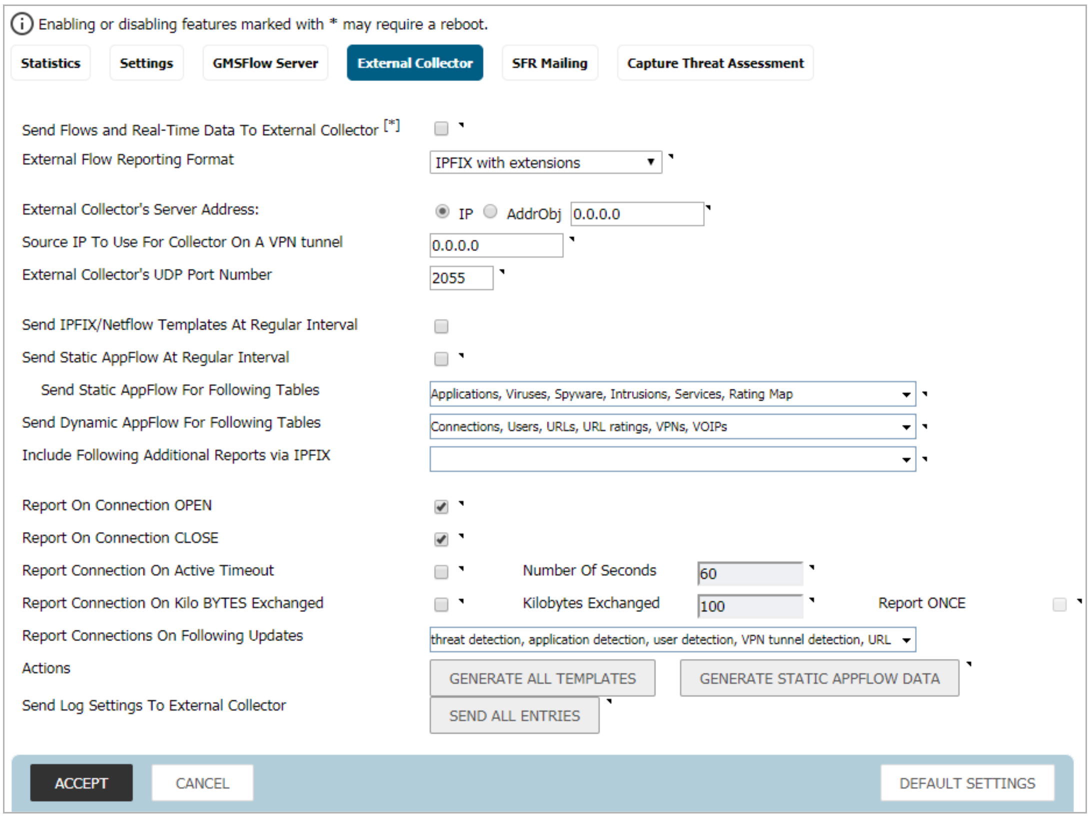
ⓘ Enabling or disabling features marked with * may require a reboot.

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**.



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

Send Flows and Real-Time Data To External Collector [*]	□
External Flow Reporting Format	IPFIX with extensions
External Collector's Server Address:	● IP ○ AddrObj 0.0.0.0
Source IP To Use For Collector On A VPN tunnel	0.0.0.0
External Collector's UDP Port Number	2055
Send IPFIX/Netflow Templates At Regular Interval	□
Send Static AppFlow At Regular Interval	□
Send Static AppFlow For Following Tables	Applications, Viruses, Spyware, Intrusions, Services, Rating Map
Send Dynamic AppFlow For Following Tables	Connections, Users, URLs, URL ratings, VPNs, VOIPs
Include Following Additional Reports via IPFIX	
Report On Connection OPEN	☑
Report On Connection CLOSE	☑
Report Connection On Active Timeout	□ Number Of Seconds 60
Report Connection On Kilo BYTES Exchanged	□ Kilobytes Exchanged 100 Report ONCE □
Report Connections On Following Updates	threat detection, application detection, user detection, VPN tunnel detection, URL
Actions	GENERATE ALL TEMPLATES GENERATE STATIC APPFLOW DATA
Send Log Settings To External Collector	SEND ALL ENTRIES

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

ⓘ **IMPORTANT:** When enabling this option, you might 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.

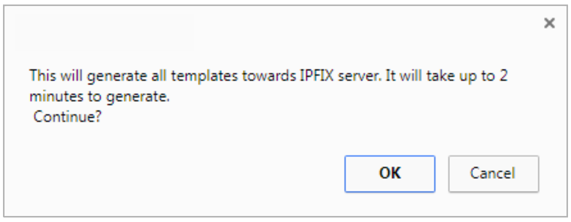
11 Select any additional reports to be generated to a flow from the **Include Following Additional Reports via IPFIX** drop-down menu.

ⓘ **IMPORTANT:** To have system logs generated, you must select System Logs from this drop-down menu.

12 Click **Generate ALL Templates** to begin generating templates.

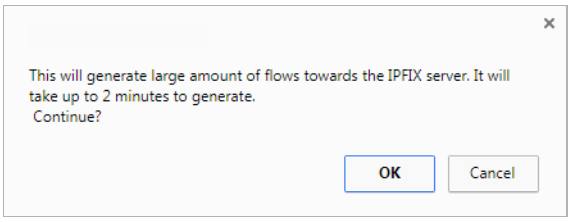
ⓘ **IMPORTANT:** IPFIX with extensions uses templates that must be known to an external collector before sending data.

13 Enable the option to **Send Static AppFlow at Regular Intervals** by selecting the checkbox. After enabling this option, click **Generate Static Flows**.



This will generate all templates towards IPFIX server. It will take up to 2 minutes to generate.
Continue?

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



This will generate large amount of flows towards the IPFIX server. It will take up to 2 minutes to generate.
Continue?

15 To send log messages to the external collector, click **Send All Entries** 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 **Send All Entries**.

The external server loads the properties (see Saved properties) and settings for use when it reboots. Click **Send All Entries** 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 might 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

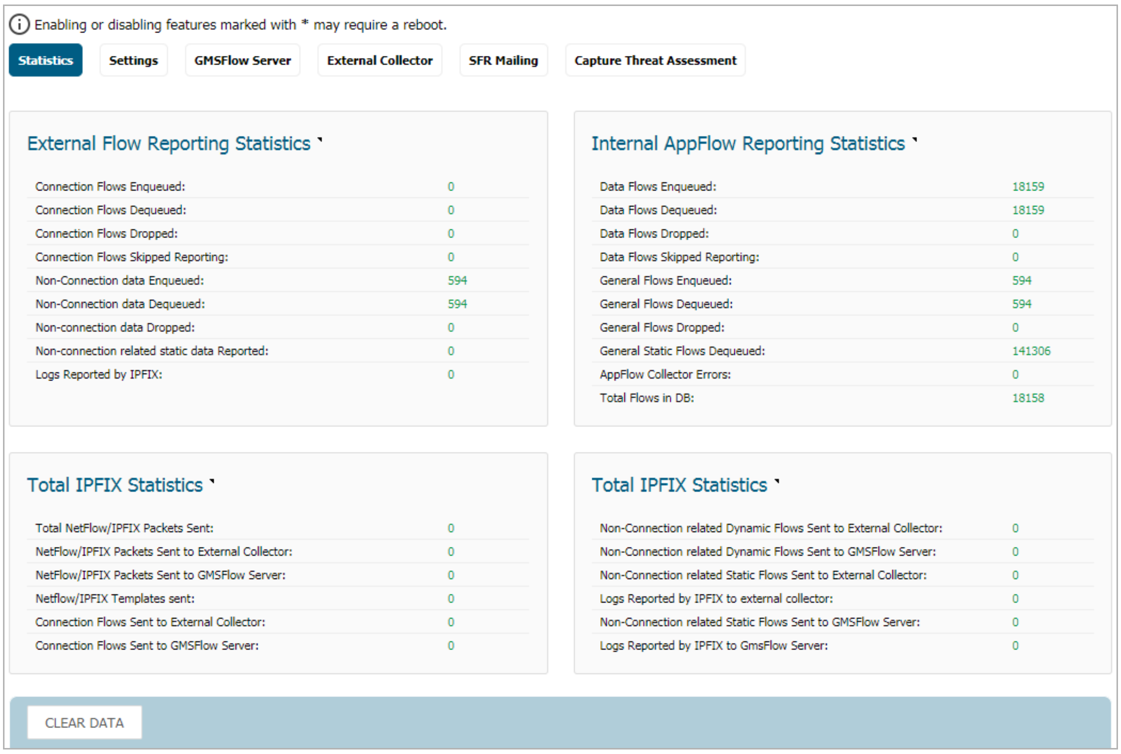
Category	Property	
Event properties and settings	Event ID Belongs to group ID Color Message type ID	Priority Stream filter Event name Log message
Group properties	Group ID Belongs to category ID	Group name
Category properties	Category ID	Category name
Message type properties	Type ID	Type name

16 Click **Accept**.

Configuring GMSFlow Server to Include Logs Through IPFIX

To configure GMSFlow server to include logs through IPFIX:

1 Navigate to **AppFlow > Flow Reporting**.



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

External Flow Reporting Statistics *

Connection Flows Enqueued:	0
Connection Flows Dequeued:	0
Connection Flows Dropped:	0
Connection Flows Skipped Reporting:	0
Non-Connection data Enqueued:	594
Non-Connection data Dequeued:	594
Non-connection data Dropped:	0
Non-connection related static data Reported:	0
Logs Reported by IPFIX:	0

Internal AppFlow Reporting Statistics *

Data Flows Enqueued:	18159
Data Flows Dequeued:	18159
Data Flows Dropped:	0
Data Flows Skipped Reporting:	0
General Flows Enqueued:	594
General Flows Dequeued:	594
General Flows Dropped:	0
General Static Flows Dequeued:	141306
AppFlow Collector Errors:	0
Total Flows in DB:	18158

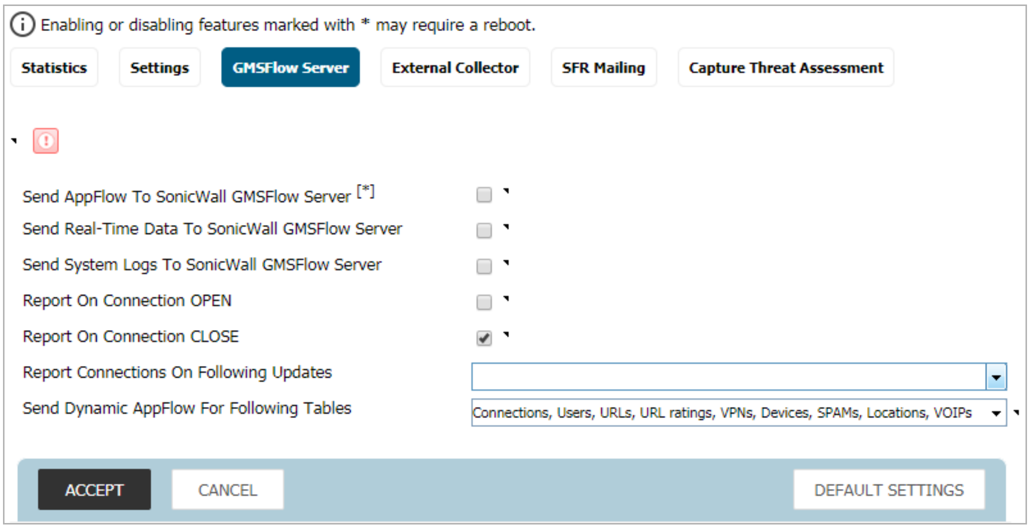
Total IPFIX Statistics *

Total NetFlow/IPFIX Packets Sent:	0
NetFlow/IPFIX Packets Sent to External Collector:	0
NetFlow/IPFIX Packets Sent to GMSFlow Server:	0
Netflow/IPFIX Templates sent:	0
Connection Flows Sent to External Collector:	0
Connection Flows Sent to GMSFlow Server:	0

Total IPFIX Statistics *

Non-Connection related Dynamic Flows Sent to External Collector:	0
Non-Connection related Dynamic Flows Sent to GMSFlow Server:	0
Non-Connection related Static Flows Sent to External Collector:	0
Logs Reported by IPFIX to external collector:	0
Non-Connection related Static Flows Sent to GMSFlow Server:	0
Logs Reported by IPFIX to GmsFlow Server:	0

2 Click **GMSFlow Server**.



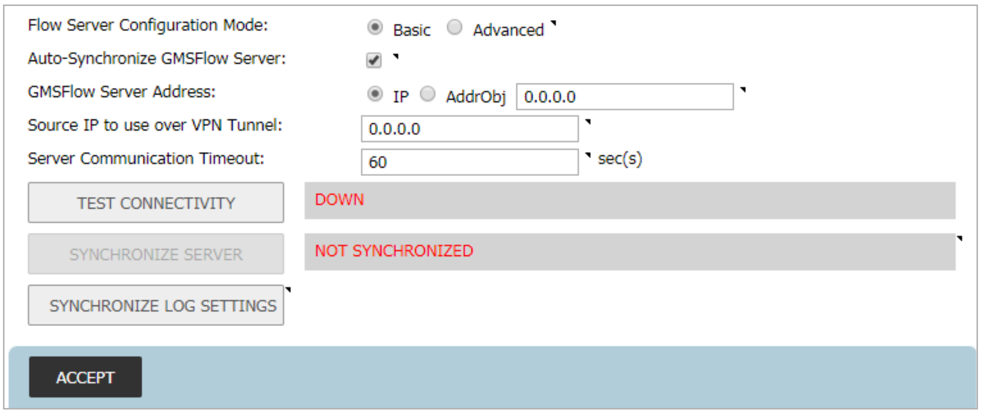
Enabling or disabling features marked with * may require a reboot.

Send AppFlow To SonicWall GMSFlow Server [*] □
Send Real-Time Data To SonicWall GMSFlow Server □
Send System Logs To SonicWall GMSFlow Server □
Report On Connection OPEN □
Report On Connection CLOSE ☑
Report Connections On Following Updates
Send Dynamic AppFlow For Following Tables: Connections, Users, URLs, URL ratings, VPNs, Devices, SPAMs, Locations, VOIPs

3 Select S**end System Logs to SonicWall GMSFlow Server**. This option is not selected by default.

4 Click **Accept**.

5 Navigate to **AppFlow Settings > GMS Flow Server**.



Flow Server Configuration Mode: ● Basic ○ Advanced
Auto-Synchronize GMSFlow Server: ☑
GMSFlow Server Address: ● IP ○ AddrObj 0.0.0.0
Source IP to use over VPN Tunnel: 0.0.0.0
Server Communication Timeout: 60 sec(s)
TEST CONNECTIVITY DOWN
SYNCHRONIZE SERVER NOT SYNCHRONIZED

6 To send log messages to the GMSFlow server, click **Synchronize Log Settings**.

> **IMPORTANT:** Ensure the connection between SonicOS on the firewall and the GMSFlow server is ready before clicking **Synchronize Log Settings**.

The external server loads the properties (see Saved properties) and settings for use when it reboots. Click **Send All Entries** 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 might have been edited during that time.

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

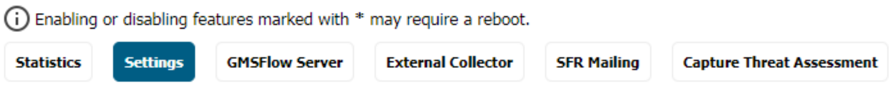
7 Click **Accept**.

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**.

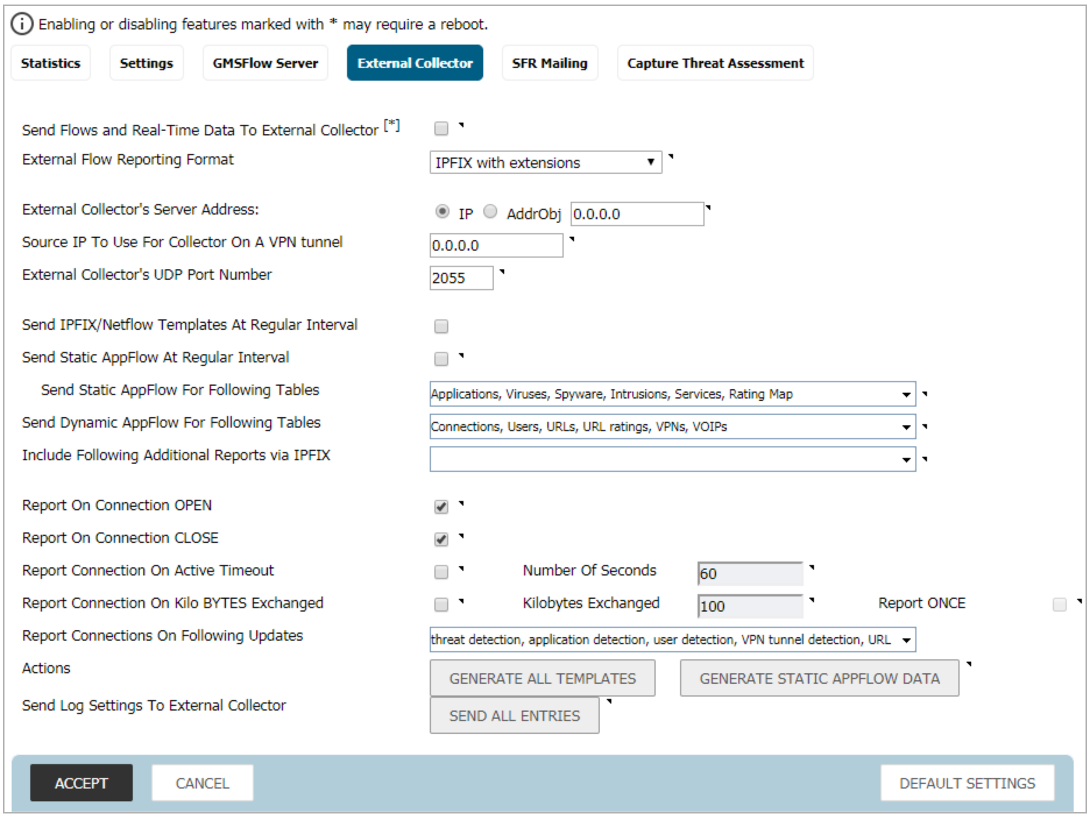


ⓘ Enabling or disabling features marked with * may require a reboot.

2 In the **Settings** section, for **Report Connections**, select **All**.

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

3 Click **External Collector**.



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

Send Flows and Real-Time Data To External Collector [*]	□
External Flow Reporting Format	IPFIX with extensions
External Collector's Server Address:	● IP ○ AddrObj 0.0.0.0
Source IP To Use For Collector On A VPN tunnel	0.0.0.0
External Collector's UDP Port Number	2055
Send IPFIX/Netflow Templates At Regular Interval	□
Send Static AppFlow At Regular Interval	□
Send Static AppFlow For Following Tables	Applications, Viruses, Spyware, Intrusions, Services, Rating Map
Send Dynamic AppFlow For Following Tables	Connections, Users, URLs, URL ratings, VPNs, VOIPs
Include Following Additional Reports via IPFIX	
Report On Connection OPEN	☑
Report On Connection CLOSE	☑
Report Connection On Active Timeout	□ Number Of Seconds 60
Report Connection On Kilo BYTES Exchanged	□ Kilobytes Exchanged 100 Report ONCE □
Report Connections On Following Updates	threat detection, application detection, user detection, VPN tunnel detection, URL
Actions	GENERATE ALL TEMPLATES GENERATE STATIC APPFLOW DATA
Send Log Settings To External Collector	SEND ALL ENTRIES

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

> ⓘ **IMPORTANT:** When enabling this option, you might 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.

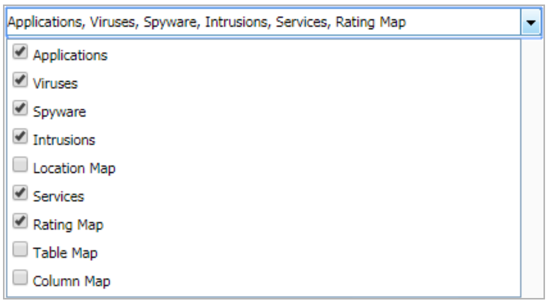
7 Optionally, if the external collector must be reached by a VPN tunnel, specify the source IP in the **Source IP to Use for Collector on a VPN Tunnel** field.

> ⓘ **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 **Send Static AppFlow At Regular Interval**.

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



Applications, Viruses, Spyware, Intrusions, Services, Rating Map

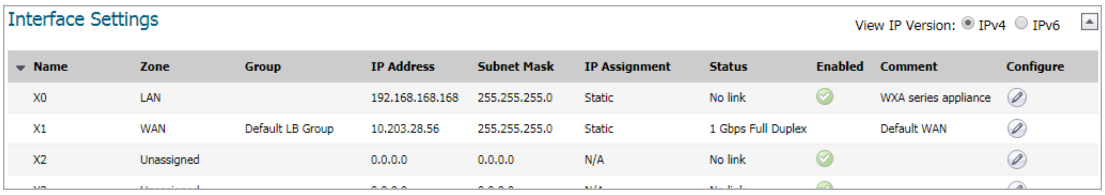
☑ Applications
☑ Viruses
☑ Spyware
☑ Intrusions
☐ Location Map
☑ Services
☑ Rating Map
☐ Table Map
☐ Column Map

> ⓘ **NOTE:** Currently, Scrutinizer supports Applications and Threats only. Future versions of Plixer supports the following Static Flows: Location Map, Services, Rating Map, Table Map, and Column Map.

11 Click **Generate Static AppFlow Data**.

12 Click **Accept**.

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

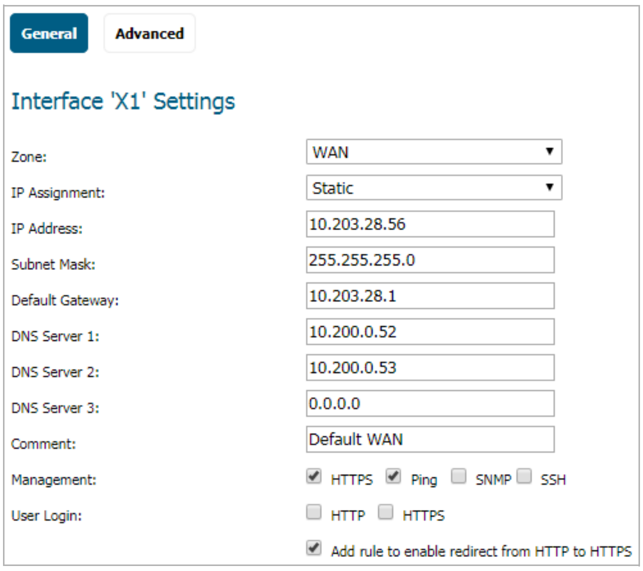


Interface Settings

View IP Version: ● IPv4 ○ IPv6

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Enabled	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	No link	✓	WXA series appliance	✎
X1	WAN	Default LB Group	10.203.28.56	255.255.255.0	Static	1 Gbps Full Duplex		Default WAN	✎
X2	Unassigned		0.0.0.0	0.0.0.0	N/A	No link	✓		✎

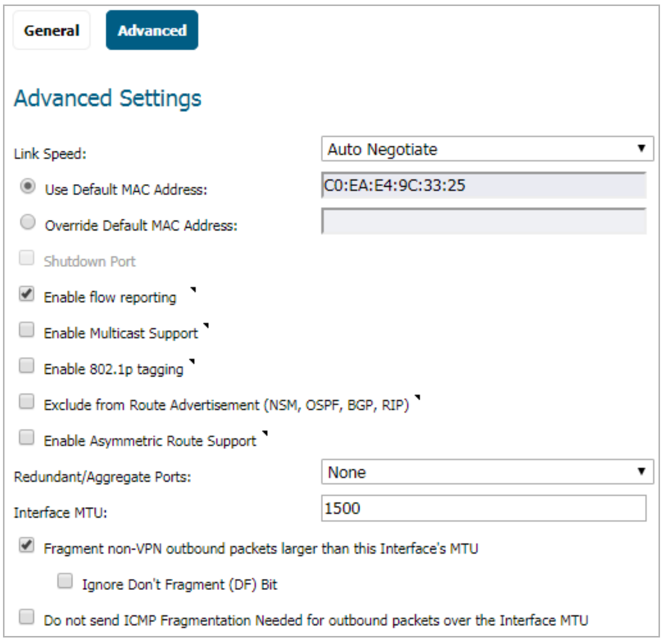
14 Confirm that Flow Reporting is enabled per interface by clicking the **Configure** icon of the interface you are requesting data from. The **Edit Interface** dialog displays.



Interface 'X1' Settings

Zone:	WAN
IP Assignment:	Static
IP Address:	10.203.28.56
Subnet Mask:	255.255.255.0
Default Gateway:	10.203.28.1
DNS Server 1:	10.200.0.52
DNS Server 2:	10.200.0.53
DNS Server 3:	0.0.0.0
Comment:	Default WAN
Management:	☑ HTTPS ☑ Ping ☐ SNMP ☐ SSH
User Login:	☐ HTTP ☐ HTTPS
	☑ Add rule to enable redirect from HTTP to HTTPS

15 On the **Advanced** screen, ensure **Enable flow reporting** is selected.



Advanced Settings

Link Speed: Auto Negotiate

● Use Default MAC Address: C0:EA:E4:9C:33:25

○ Override Default MAC Address:

□ Shutdown Port

☑ Enable flow reporting

□ Enable Multicast Support

□ Enable 802.1p tagging

□ Exclude from Route Advertisement (NSM, OSPF, BGP, RIP)

□ Enable Asymmetric Route Support

Redundant/Aggregate Ports: None

Interface MTU: 1500

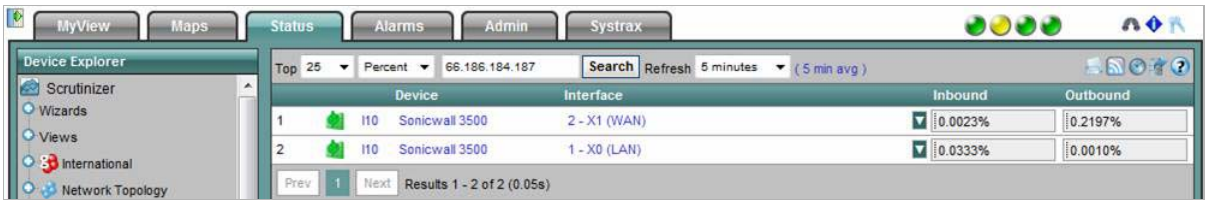
☑ Fragment non-VPN outbound packets larger than this Interface's MTU

□ Ignore Don't Fragment (DF) Bit

□ Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

16 Click **OK**.

17 Log in to SonicWall Scrutinizer. The data displays within minutes.



Top 25 Percent 66.186.184.187 Refresh 5 minutes (5 min avg)

		Device	Interface	Inbound	Outbound
1	I10	Sonicwall 3500	2 - X1 (WAN)	0.0023%	0.2197%
2	I10	Sonicwall 3500	1 - X0 (LAN)	0.0333%	0.0010%

Results 1 - 2 of 2 (0.05s)

NetFlow Tables

The following section describes the various NetFlow tables. Also, this section describes in detail the IPFX 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 might also be configured to send just once. Exportable Static IPFIX tables lists the Static IPFIX tables that might 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

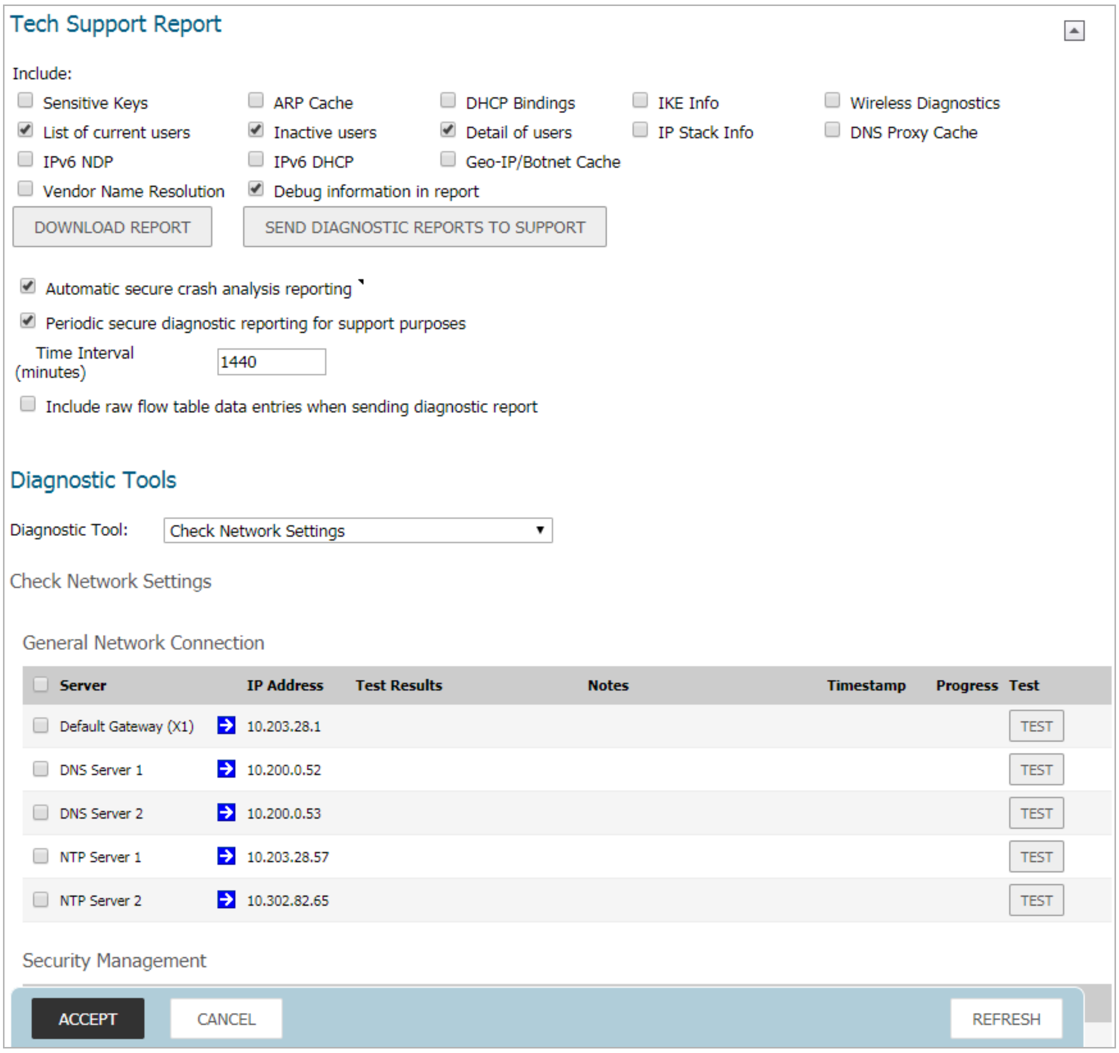
Unlike Static tables, the data of Dynamic tables change over time and are sent repeatedly, based on the activity of the firewall. The columns of these tables grow over time, with the exception of a few tables containing statistics or utilization reports. Exportable Dynamic IPFIX tables lists the Dynamic IPFIX tables that might 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 through 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 do a Diagnostic Report of your own Netflow Configuration by navigating to **INVESTIGATE | Tools | System Diagnostics**, and clicking **Download Report** in the **Tech Support Report** section.



Tech Support Report

Include:

☐ Sensitive Keys ☐ ARP Cache ☐ DHCP Bindings ☐ IKE Info ☐ Wireless Diagnostics
☑ List of current users ☑ Inactive users ☑ Detail of users ☐ IP Stack Info ☐ DNS Proxy Cache
☐ IPv6 NDP ☐ IPv6 DHCP ☐ Geo-IP/Botnet Cache
☐ Vendor Name Resolution ☑ Debug information in report

DOWNLOAD REPORT | SEND DIAGNOSTIC REPORTS TO SUPPORT

☑ Automatic secure crash analysis reporting

☑ Periodic secure diagnostic reporting for support purposes

Time Interval (minutes): 1440

☐ Include raw flow table data entries when sending diagnostic report

Diagnostic Tools

Diagnostic Tool: Check Network Settings

Check Network Settings

General Network Connection

☐ Server	IP Address	Test Results	Notes	Timestamp	Progress	Test
☐ Default Gateway (X1)	10.203.28.1					TEST
☐ DNS Server 1	10.200.0.52					TEST
☐ DNS Server 2	10.200.0.53					TEST
☐ NTP Server 1	10.203.28.57					TEST
☐ NTP Server 2	10.302.82.65					TEST

Security Management

ACCEPT | CANCEL | REFRESH

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 that 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

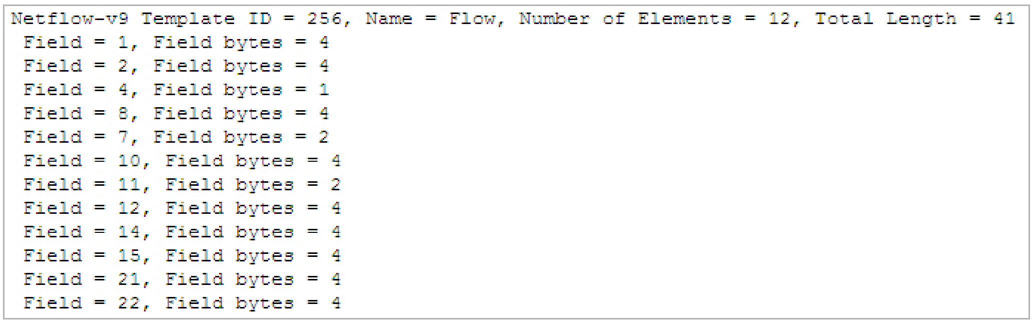
Bytes	Contents	Description
0-1	version	NetFlow export format version number
2-3	count	Number of flows exported in this packet (1-30)
4-7	SysUptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds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

Netflow Version 5 Record Format

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

NetFlow Version 9

NetFlow Version 9 Example



```
Netflow-v9 Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 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
```

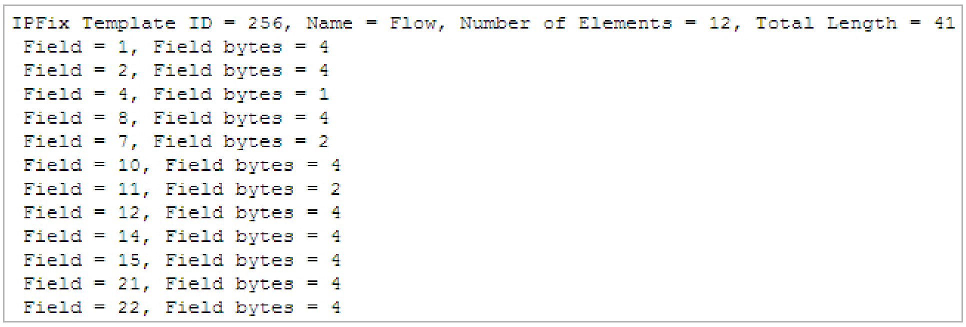
Netflow Version 9 Template FlowSet Fields details the NetFlow version 9 Template FlowSet field descriptions.

Netflow Version 9 Template FlowSet Fields

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

IPFIX (NetFlow Version 10)

IPFIX (NetFlow Version 10) Example



```
IPFix Template ID = 256, Name = Flow, Number of Elements = 12, Total Length = 41
 Field = 1, Field bytes = 4
 Field = 2, Field bytes = 4
 Field = 4, Field bytes = 1
 Field = 8, Field bytes = 4
 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

Field Name	Description
Template ID	The firewall generates templates with a unique ID based on FlowSet templates matching the type of NetFlow data being exported.
Name	The name of the NetFlow template.
Number of Elements	The amount of fields listed in the NetFlow template.

IPFIX template FlowSet fields

Field Name	Description
Total Length	The total length in bytes of all reported fields in the NetFlow template.
Field Type	The field type is a numeric value that represents the type of field. Note that values of the field type might be vendor specific.
Field bytes	The length of the specific Field Type, in bytes.

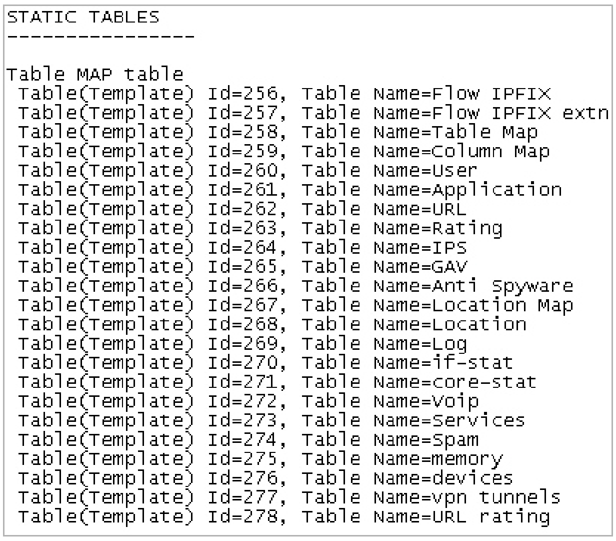
IPFIX with Extensions

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.

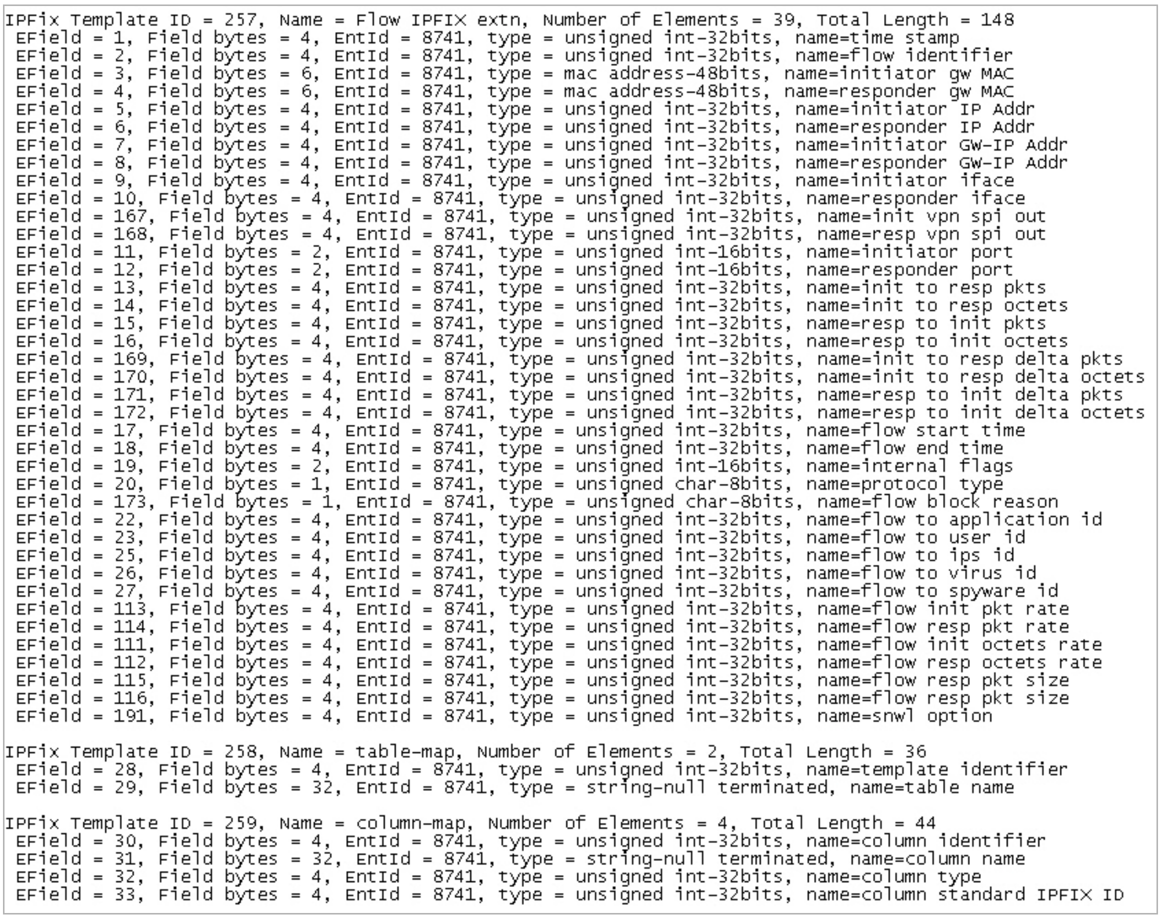
IPFIX with Extensions Name Template Example is a standard for the IPFIX with extensions templates. The values specified are static and correlate to the Table Name of all the NetFlow exportable templates. Also see IPFIX with Extensions Template Example.

IPFIX with Extensions Name Template Example



```
STATIC TABLES
----------------

Table MAP table
 Table(Template) Id=256, Table Name=Flow IPFIX
 Table(Template) Id=257, Table Name=Flow IPFIX extn
 Table(Template) Id=258, Table Name=Table Map
 Table(Template) Id=259, Table Name=Column Map
 Table(Template) Id=260, Table Name=User
 Table(Template) Id=261, Table Name=Application
 Table(Template) Id=262, Table Name=URL
 Table(Template) Id=263, Table Name=Rating
 Table(Template) Id=264, Table Name=IPS
 Table(Template) Id=265, Table Name=GAV
 Table(Template) Id=266, Table Name=Anti Spyware
 Table(Template) Id=267, Table Name=Location Map
 Table(Template) Id=268, Table Name=Location
 Table(Template) Id=269, Table Name=Log
 Table(Template) Id=270, Table Name=if-stat
 Table(Template) Id=271, Table Name=core-stat
 Table(Template) Id=272, Table Name=Voip
 Table(Template) Id=273, Table Name=Services
 Table(Template) Id=274, Table Name=Spam
 Table(Template) Id=275, Table Name=memory
 Table(Template) Id=276, Table Name=devices
 Table(Template) Id=277, Table Name=vpn tunnels
 Table(Template) Id=278, Table Name=URL rating
```

IPFIX with Extensions Template Example

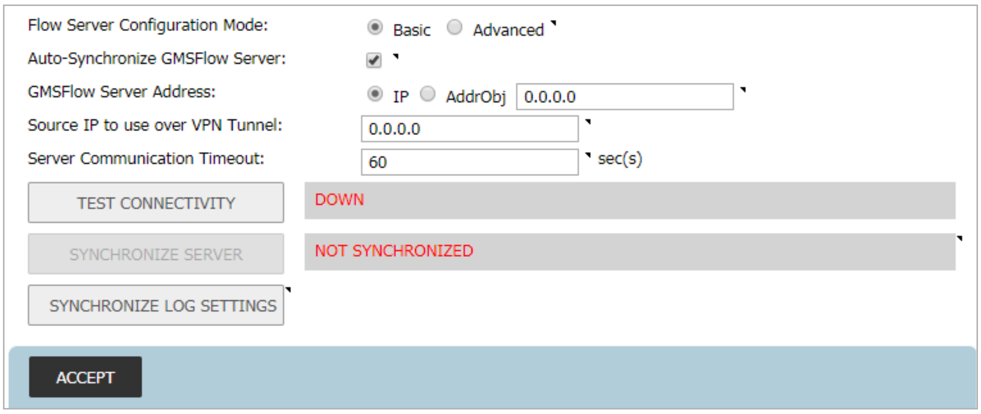


```
IPFix Template ID = 257, Name = Flow IPFIX extn, Number of Elements = 39, Total Length = 148
 EField = 1, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=time stamp
 EField = 2, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow identifier
 EField = 3, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=initiator gw MAC
 EField = 4, Field bytes = 6, EntId = 8741, type = mac address-48bits, name=responder gw MAC
 EField = 5, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator IP Addr
 EField = 6, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder IP Addr
 EField = 7, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator GW-IP Addr
 EField = 8, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder GW-IP Addr
 EField = 9, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=initiator iface
 EField = 10, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=responder iface
 EField = 167, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init vpn spi out
 EField = 168, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp vpn spi out
 EField = 11, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=initiator port
 EField = 12, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=responder port
 EField = 13, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp pkts
 EField = 14, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp octets
 EField = 15, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init pkts
 EField = 16, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init octets
 EField = 169, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta pkts
 EField = 170, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=init to resp delta octets
 EField = 171, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta pkts
 EField = 172, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=resp to init delta octets
 EField = 17, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow start time
 EField = 18, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow end time
 EField = 19, Field bytes = 2, EntId = 8741, type = unsigned int-16bits, name=internal flags
 EField = 20, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=protocol type
 EField = 173, Field bytes = 1, EntId = 8741, type = unsigned char-8bits, name=flow block reason
 EField = 22, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to application id
 EField = 23, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to user id
 EField = 25, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to ips id
 EField = 26, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to virus id
 EField = 27, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow to spyware id
 EField = 113, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init pkt rate
 EField = 114, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt rate
 EField = 111, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow init octets rate
 EField = 112, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp octets rate
 EField = 115, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 116, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=flow resp pkt size
 EField = 191, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=snwl option

IPFix Template ID = 258, Name = table-map, Number of Elements = 2, Total Length = 36
 EField = 28, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=template identifier
 EField = 29, Field bytes = 32, EntId = 8741, type = string-null terminated, name=table name

IPFix Template ID = 259, Name = column-map, Number of Elements = 4, Total Length = 44
 EField = 30, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column identifier
 EField = 31, Field bytes = 32, EntId = 8741, type = string-null terminated, name=column name
 EField = 32, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column type
 EField = 33, Field bytes = 4, EntId = 8741, type = unsigned int-32bits, name=column standard IPFIX ID
```

2

Connecting to a GMSFlow Server

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



Flow Server Configuration Mode:	● Basic ○ Advanced
Auto-Synchronize GMSFlow Server:	☑
GMSFlow Server Address:	● IP ○ AddrObj 0.0.0.0
Source IP to use over VPN Tunnel:	0.0.0.0
Server Communication Timeout:	60 sec(s)
TEST CONNECTIVITY	DOWN
SYNCHRONIZE SERVER	NOT SYNCHRONIZED

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 that 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 of 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.

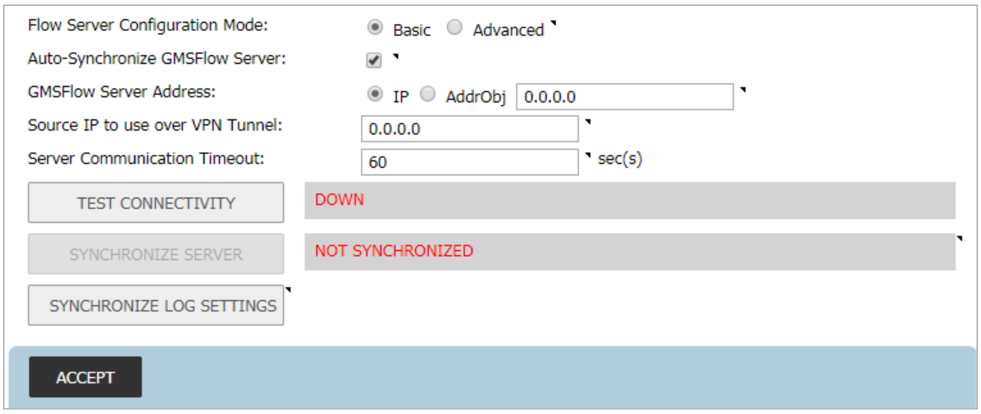
For more detailed information about configuring an AppFlow server with GMS, refer to the latest SonicWall GMS or SonicWall Management Services administration documentation, available at https://www.sonicwall.com/support/technical-documentation.

To establish a connection to a GMSFlow Server:

1. In GMS, log in to 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.



Flow Server Configuration Mode: ● Basic ○ Advanced

Auto-Synchronize GMSFlow Server: ☑

GMSFlow Server Address: ● IP ○ AddrObj 0.0.0.0

Source IP to use over VPN Tunnel: 0.0.0.0

Server Communication Timeout: 60 sec(s)

TEST CONNECTIVITY DOWN

SYNCHRONIZE SERVER NOT SYNCHRONIZED

SYNCHRONIZE LOG SETTINGS

ACCEPT

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** drop-down menu. 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 through 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 waits 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 **Test Connectivity**. The connectivity status is displayed.

8 If you want to manually send static data to the GMSFlow Server, click **Synchronize Server**. The synchronicity status is displayed.

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

9 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 or SonicWall Management Services administration documentation, available at https://www.sonicwall.com/support/technical-documentation.

To establish a connection to a GMSFlow Server:

1 In GMS, log in to the Instant GMSFlow Server.

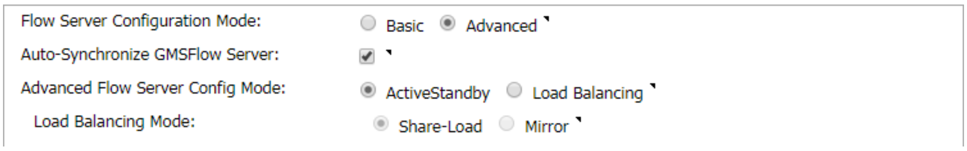
2 Go to the **Network** > **Settings** page.

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**.



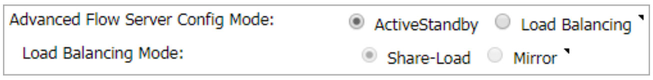
Flow Server Configuration Mode: ○ Basic ● Advanced

Auto-Synchronize GMSFlow Server: ☑

Advanced Flow Server Config Mode: ● ActiveStandby ○ Load Balancing

Load Balancing Mode: ● Share-Load ○ Mirror

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



Advanced Flow Server Config Mode: ● ActiveStandby ○ Load Balancing

Load Balancing Mode: ● Share-Load ○ Mirror

- **ActiveStandby** — If you select this option, flows are directed first to GMSFlow Server 1 (if available). If GMSFlow Server 1 is not available, flows are 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 are divided equally between the two flow servers.
        - **Mirror** — If you select this load-balancing option, all flows are 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** drop-down menu. 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 through 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 waits 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 **Test Connectivity** for that GMSFlow Server. The connectivity status is displayed.

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

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

10 Click **Accept**.

Topics:

- Connecting to a GMSFlow Server
- Basic Mode

Part 2

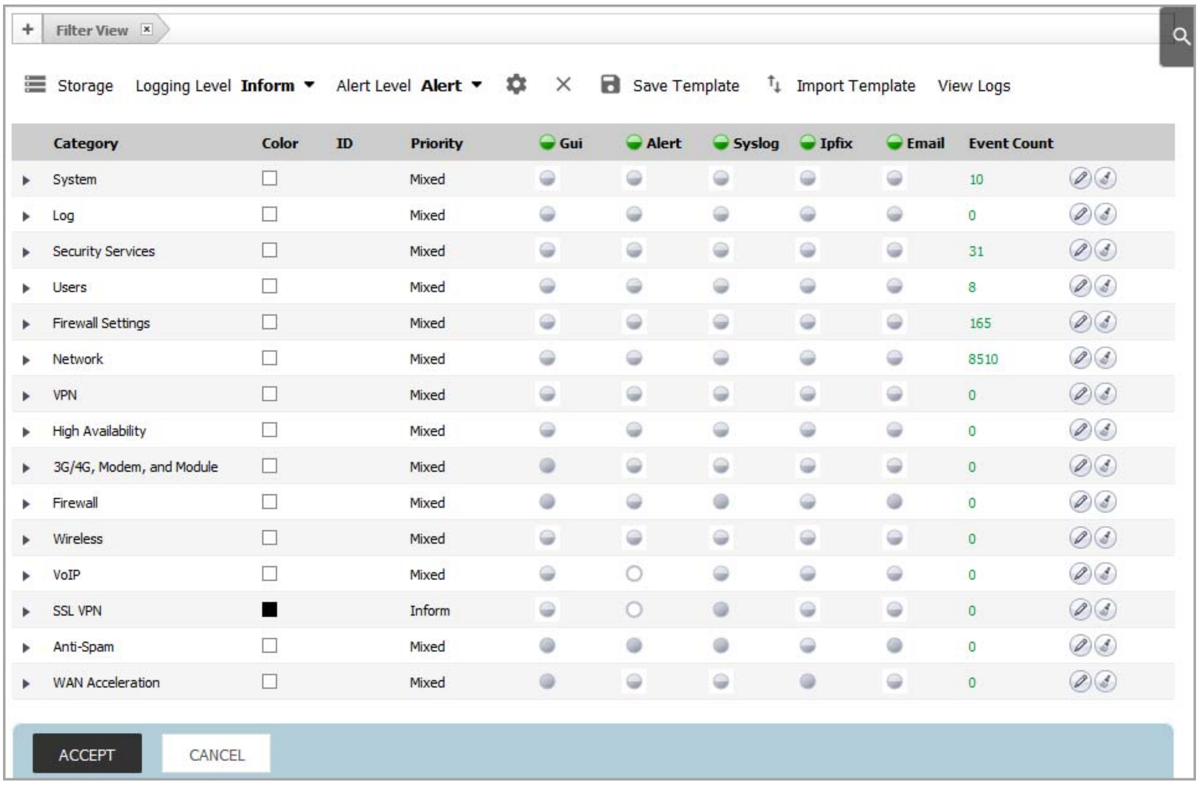
Logs & Reporting | Log Settings

3

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.

Log Settings > Base Setup page



	Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count
▸	System	□		Mixed	●	●	●	●	●	10
▸	Log	□		Mixed	●	●	●	●	●	0
▸	Security Services	□		Mixed	●	●	●	●	●	31
▸	Users	□		Mixed	●	●	●	●	●	8
▸	Firewall Settings	□		Mixed	●	●	●	●	●	165
▸	Network	□		Mixed	●	●	●	●	●	8510
▸	VPN	□		Mixed	●	●	●	●	●	0
▸	High Availability	□		Mixed	●	●	●	●	●	0
▸	3G/4G, Modem, and Module	□		Mixed	●	●	●	●	●	0
▸	Firewall	□		Mixed	●	●	●	●	●	0
▸	Wireless	□		Mixed	●	●	●	●	●	0
▸	VoIP	□		Mixed	●	○	●	●	●	0
▸	SSL VPN	■		Inform	●	○	●	●	●	0
▸	Anti-Spam	□		Mixed	●	●	●	●	●	0
▸	WAN Acceleration	□		Mixed	●	●	●	●	●	0

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

Topics:

- Filtering the Base Setup View on page 49
- Setting Storage Options on page 50
- Configuring the Logging and Alert Levels on page 52
- About Other Top Row Buttons on page 55
- About the Log Settings Base Setup Table on page 58
- Configuring Event Attributes Globally on page 63
- Configuring Event Attributes Selectively on page 66

Filtering the Base Setup View

You can create filters for log data by using the **Filter View** field on the **Log Settings > Base Setup** page to create a filter at the category, group, or event level. This provides a way to filter the display of **Log Settings > Base Setup** to make it easier to view settings of selected events. The Filter View in this context only allows "name, priority, id." You can create simple or complex filters, depending on the criteria you specify.

Log data is displayed on the **INVESTIGATE | Logs > Event Logs** page that has its own Filter View that is more granular. You can display the **INVESTIGATE | Logs > Event Logs** page quickly by clicking **View Logs** in the top row of the **Log Settings > Base Setup** page. For information about the **INVESTIGATE** view, see the *SonicWall SonicOS 6.5 Investigate* administration documentation.

Topics:

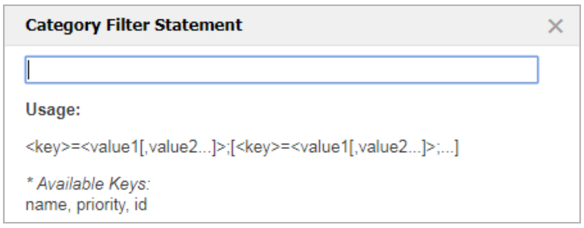
- Adding a Filter
- Viewing a Filter
- Deleting a Filter

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.
>
> You can click the ⧉ icon at the top of the page to display this page in a new browser tab. This allows you to maintain your filter view while navigating to other SonicOS pages in the other browser tab.

To create a filter using Filter View:

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

   Category Filter Statement

   Usage:

   <key>=<value1[,value2...]>;[<key>=<value1[,value2...]>;...]

   ** Available Keys:*
   name, priority, id

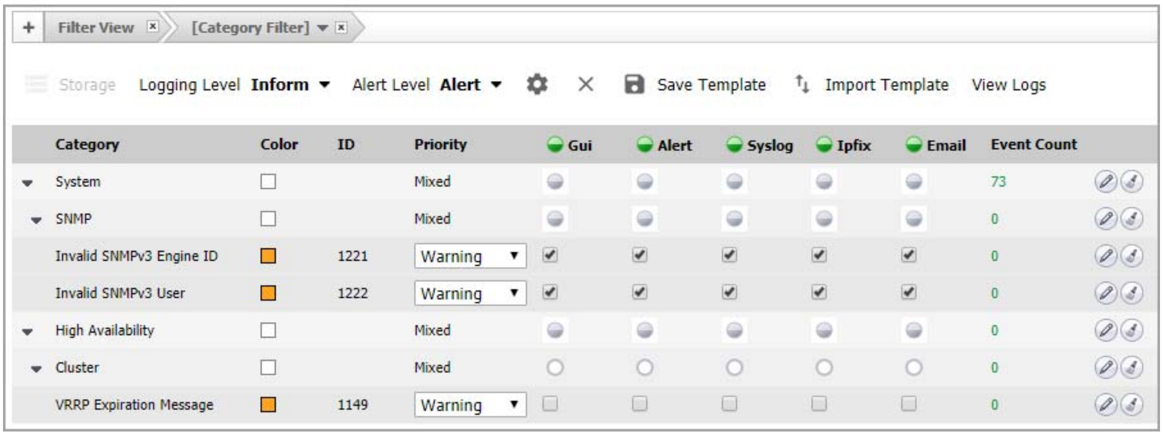
2. Enter the filter. For example, `priority=Warning;id=1221;id=1222;id=1149`. You can enter multiple keys separated by a semicolon (;) and for each key, multiple values separated by a comma. A key can be a **name** (from the whole table), **priority** (from Priority), or **ID** (from the ID column).

   The **name** keyword does a general search on the table, is case insensitive, and supports partial matches. For **priority**, the search is done on the **Priority** column only and the key must be the full word with proper capitalization (case sensitive). For example, `priority=warn` does NOT work but `priority=Warning` works.

   > **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, **[Category Filter]**, appears next to **Filter View**:

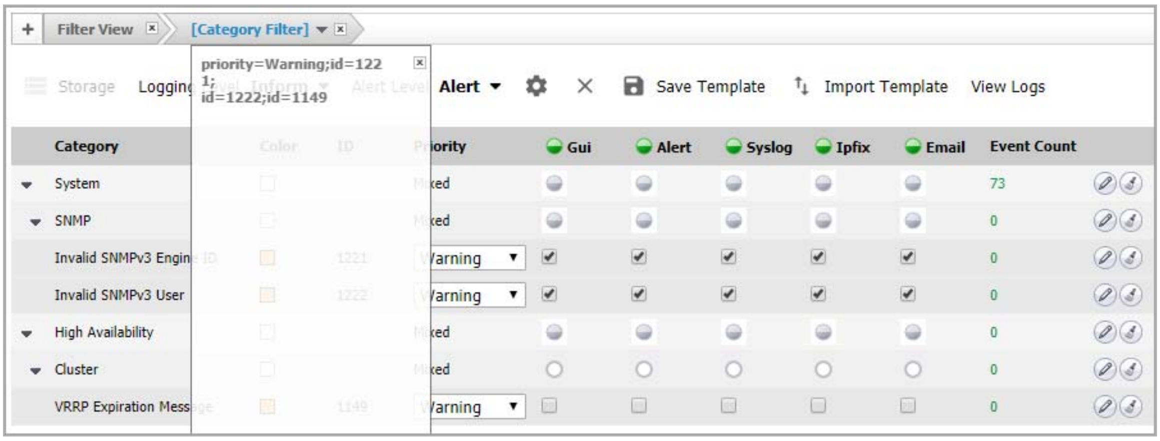


Logging Level **Inform** ▾ Alert Level **Alert** ▾

	Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count	
▾	System	□		Mixed	●	●	●	●	●	73	
▾	SNMP	□		Mixed	●	●	●	●	●	0	
	Invalid SNMPv3 Engine ID	🟧	1221	Warning ▾	☑	☑	☑	☑	☑	0	
	Invalid SNMPv3 User	🟧	1222	Warning ▾	☑	☑	☑	☑	☑	0	
▾	High Availability	□		Mixed	●	●	●	●	●	0	
▾	Cluster	□		Mixed	○	○	○	○	○	0	
	VRRP Expiration Message	🟧	1149	Warning ▾	□	□	□	□	□	0	

Viewing a Filter

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



priority=Warning;id=122
1;
id=1222;id=1149

Logging Level Inform ▾ Alert Level **Alert** ▾

	Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count	
▾	System			Mixed	●	●	●	●	●	73	
▾	SNMP			Mixed	●	●	●	●	●	0	
	Invalid SNMPv3 Engine ID		1221	Warning ▾	☑	☑	☑	☑	☑	0	
	Invalid SNMPv3 User		1222	Warning ▾	☑	☑	☑	☑	☑	0	
▾	High Availability			Mixed	●	●	●	●	●	0	
▾	Cluster			Mixed	○	○	○	○	○	0	
	VRRP Expiration Message		1149	Warning ▾	□	□	□	□	□	0	

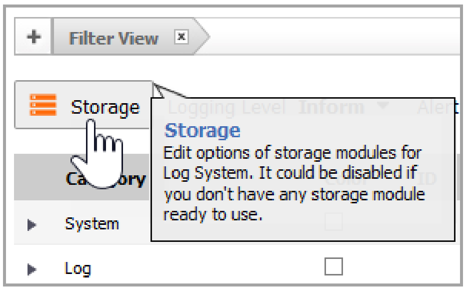
ⓘ **NOTE:** To close the pop-up, click **[Category Filter]** again. Do not click the **X** in the upper right corner of the pop-up as doing so deletes the filter.

Deleting a Filter

To delete a filter, click on the **X** in **Filter View**, the **[Category Filter]** button, or the pop-up display. Displaying another page or logging out also deletes the filter.

Setting Storage Options

Storage 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. **Storage** also provides a way to purge all files from either storage module.



Storage
Edit options of storage modules for Log System. It could be disabled if you don't have any storage module ready to use.

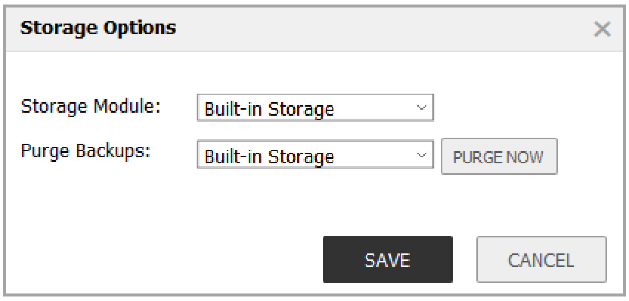
Storage is disabled if your security appliance does not have any available storage modules.

Unlike Built-in Storage that 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 **Storage** at the top, above the table. The **Storage Options** dialog displays.



Storage Options

Storage Module: Built-in Storage

Purge Backups: Built-in Storage

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

Purging a Storage Module

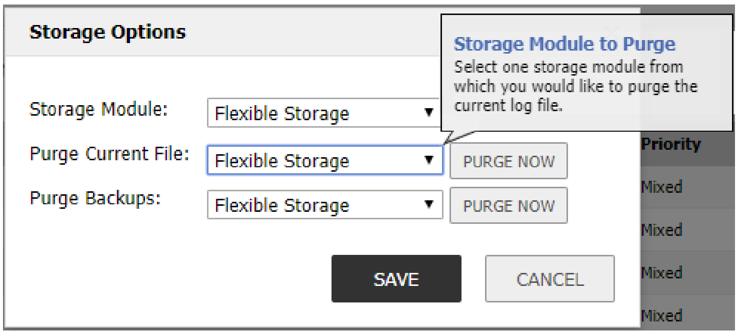
Purging a storage module removes all the data from it.

To purge a storage module:

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

3 To purge the current log file from the storage module, select the storage module to purge from the **Purge Current File** drop-down menu.

4 To purge all backups from the storage module, select the storage module to purge from the **Purge Backups** drop-down menu.



Storage Options

Storage Module: Flexible Storage ▾

Purge Current File: Flexible Storage ▾

Purge Backups: Flexible Storage ▾

Storage Module to Purge
Select one storage module from which you would like to purge the current log file.

5 Click **PURGE NOW**. A confirmation dialog displays.

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

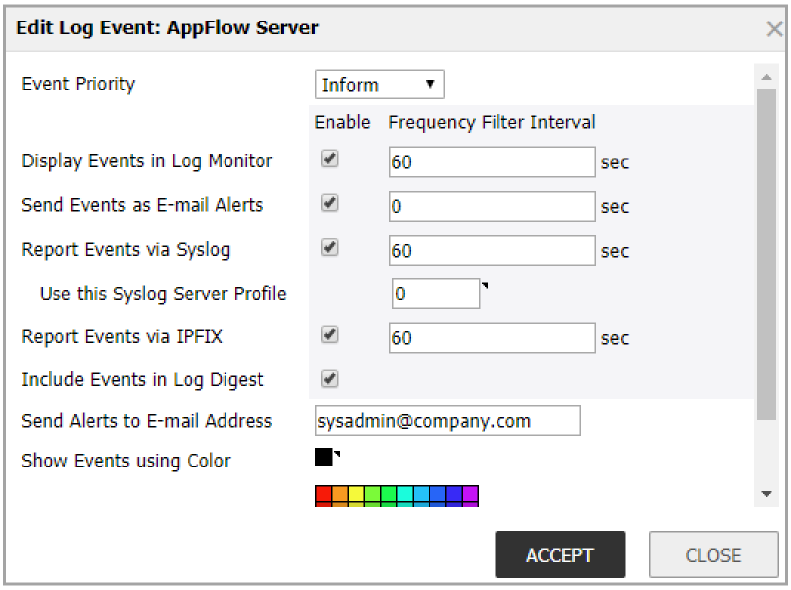
7 Click **CANCEL** or the **X** to close the **Storage Options** dialog.

Configuring the Logging and Alert Levels

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

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

- The **Enable** checkbox for **Send Events as E-mail Alerts** is selected in the **Edit Log Event** dialog launched from the table on the **Log Settings > Base Setup** page.



Edit Log Event: AppFlow Server

Event Priority: Inform ▾

	Enable	Frequency Filter Interval
Display Events in Log Monitor	☑	60 sec
Send Events as E-mail Alerts	☑	0 sec
Report Events via Syslog	☑	60 sec
Use this Syslog Server Profile		0
Report Events via IPFIX	☑	60 sec
Include Events in Log Digest	☑	

Send Alerts to E-mail Address: sysadmin@company.com

Show Events using Color: ■

- There is an email address configured in **Send Alerts to E-mail Address** in the **Log Settings > Automation** page or in one of the ***Edit*** dialogs launched from the table on **Log Settings > Base Setup**:
  - **Edit Log Category** dialog

- **Edit Log Group** dialog
- **Edit Log Event** dialog

Topics:

- Setting the Logging Level
- Setting the Alert Level

Setting the Logging Level

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

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

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

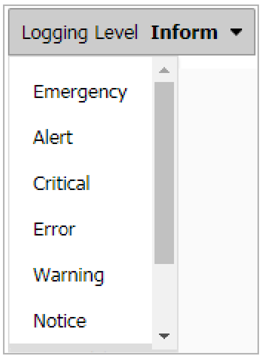
- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Inform**
- **Debug**

The default level is **Inform**.

To set the logging level:

1 Navigate to the **Logs & Reporting | Log Settings** > **Base Setup** page.

2 From the **Logging Level** drop-down menu, select the logging level you want.



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

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

Setting the Alert Level

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

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

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

The following alert levels are available for selection:

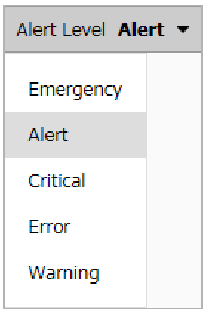
- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**

The default value is **Alert**.

To set the alert level:

1 Navigate to the **Logs & Reporting | Log Settings** > **Base Setup** page.

2 From the **Alert Level** drop-down menu, select the alert level you want.

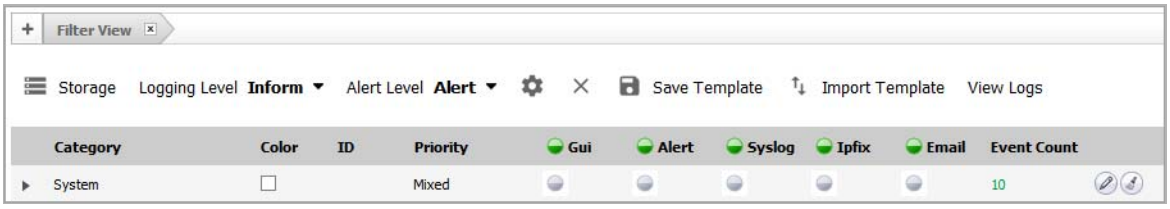


All events with **Event Priority** equal to or higher than the selected **Alert Level** are also emailed. For example, if you select ***Error*** as the **Alert Level**, all messages all messages with **Event Priority** of ***Error***, ***Critical***, ***Alert***, and ***Emergency*** are emailed.

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

About Other Top Row Buttons

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



Topics:

- Edit Attributes of All Categories Button
- Reset Event Count Button
- Save Template Button
- Import Template Button
- View Logs Button

Edit Attributes of All Categories Button

Clicking the **Configure** icon ⚙ above the table launches the **Edit Attributes of All Categories** dialog. This dialog enables you to set the attributes for all events in all categories and groups at once. For information about this procedure, refer to Configuring Event Attributes Globally on page 63.

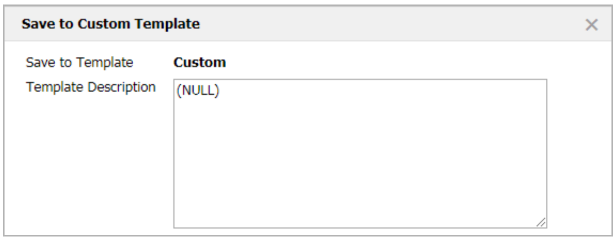
Reset Event Count Button

Reset Event Count ✕ sets **all** the event counters to zero (0).

Save Template Button

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

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.



Save to Custom Template

Save to Template **Custom**

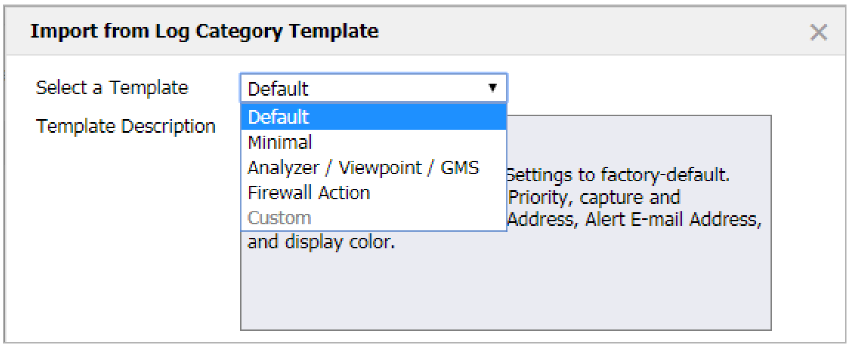
Template Description (NULL)

Import Template Button

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

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

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



Import from Log Category Template

Select a Template: Default

Template Description:
Settings to factory-default.
Priority, capture and
Address, Alert E-mail Address,
and display color.

+++++++++++++++++++++++

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

Topics:

- Default Template
- Minimal Template

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

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

Default Template

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

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

Minimal Template

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

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

Analyzer/Viewpoint/GMS Template

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

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

- Report Events via Syslog
- Frequency Filter Interval for Syslog

Firewall Action Template

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

Custom Template

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

View Logs Button

View Logs in the top row of the **Log Settings > Base Setup** page takes you to the **INVESTIGATE | Logs > Event Logs** page where you can view the log data. For information about the **INVESTIGATE** view, see the *SonicWall SonicOS 6.5 Investigate* administration documentation.

About the Log Settings Base Setup Table

Topics:

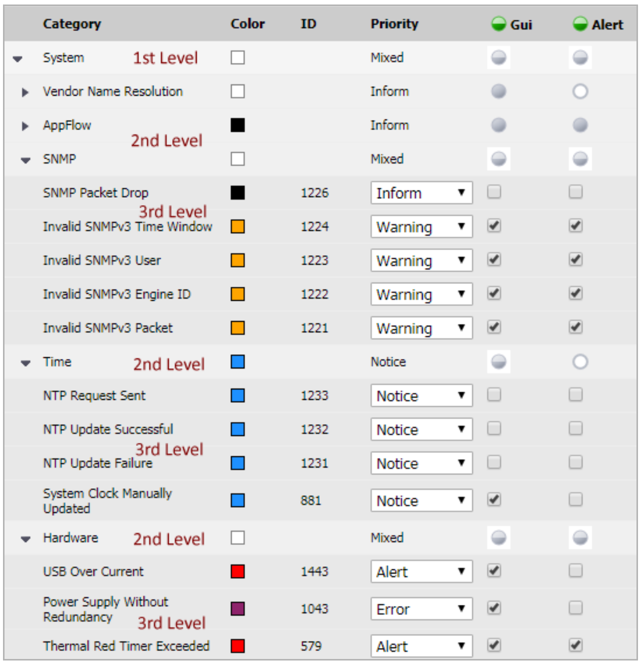
- Category Column
- Color Column
- ID Column
- Priority Column
- Gui Column
- Alert Column
- Syslog Column
- Ipfix Column
- Email Column
- Event Count Column
- Edit and Reset Event Count Icons

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:



Category	Color	ID	Priority	Gui	Alert
▼ System	□		Mixed	◐	◐
▶ Vendor Name Resolution	□		Inform	●	○
▶ AppFlow	■		Inform	●	●
▼ SNMP	□		Mixed	◐	◐
SNMP Packet Drop	■	1226	Inform ▾	□	□
Invalid SNMPv3 Time Window	🟧	1224	Warning ▾	☑	☑
Invalid SNMPv3 User	🟧	1223	Warning ▾	☑	☑
Invalid SNMPv3 Engine ID	🟧	1222	Warning ▾	☑	☑
Invalid SNMPv3 Packet	🟧	1221	Warning ▾	☑	☑
▼ Time	🟦		Notice	◐	○
NTP Request Sent	🟦	1233	Notice ▾	□	□
NTP Update Successful	🟦	1232	Notice ▾	□	□
NTP Update Failure	🟦	1231	Notice ▾	□	□
System Clock Manually Updated	🟦	881	Notice ▾	☑	□
▼ Hardware	□		Mixed	◐	◐
USB Over Current	🟥	1443	Alert ▾	☑	□
Power Supply Without Redundancy	🟪	1043	Error ▾	☑	□
Thermal Red Timer Exceeded	🟥	579	Alert ▾	☑	☑

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 Log Events Reference Guide*.

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

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

Priority Column

CAUTION: Changing the Event Priority could have serious consequences. Changing the Event Priority on the Group or Category level also changes all Events under that Group or Category to the same Event Priority value. Modifying the Event Priority affects the Syslog output for the tag "pri=" as well as how the event is treated when performing filtering by Logging Level or Alert Level. Setting the Event Priority to a level that is lower than the Logging Level causes those events to be filtered out. Also, as SonicWall GMS ignores received Syslogs that have a level of Debug, heartbeat messages and reporting messages must have a minimum Event Priority of Inform.

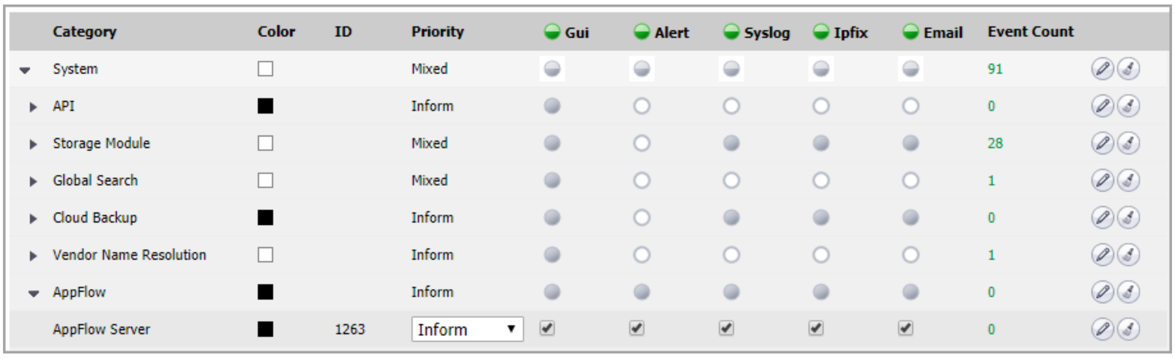
The **Priority** column shows the severity or priority of a category, group, or event. For events, a drop-down menu lists the selectable priorities. For categories and groups, the priorities are listed in the dialog when you click **Configure** at the end of the row.

The available priorities are:

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

Gui Column

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



Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count
▼ System	☐		Mixed	●	●	●	●	●	91
▶ API	■		Inform	●	○	○	○	○	0
▶ Storage Module	☐		Mixed	●	○	●	●	●	28
▶ Global Search	☐		Mixed	●	○	○	○	○	1
▶ Cloud Backup	■		Inform	●	○	●	●	●	0
▶ Vendor Name Resolution	☐		Inform	●	○	○	○	○	1
▼ AppFlow	■		Inform	●	●	●	●	●	0
AppFlow Server	■	1263	Inform ▾	☑	☑	☑	☑	☑	0

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

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

Alert Column

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

The checkbox or indicator for **Alert** applies to both sending of an email per-event and to the generation of an SNMP Trap (if SNMP configuration is enabled). For E-mail Alerts, the E-mail Address is either the global value set in the **Send Alerts to E-mail Address** field in the **Log Settings > Automation** page or the custom address configured in the **Send Alerts to E-mail Address** field in one of the ***Edit*** dialogs launched from the table on **Log Settings > Base Setup**.

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

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

Syslog Column

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

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

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

Ipfix Column

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

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

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

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

Email Column

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

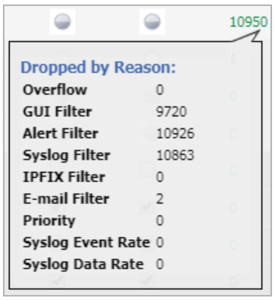
For events, these checkboxes are configurable in the column. For categories or groups, **Email** is configured in the **Edit Log Group** or **Edit Log Category** dialogs that appear when you click **Edit** at the end of the row.

Event Count Column

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

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

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



10950

Dropped by Reason:

Overflow	0
GUI Filter	9720
Alert Filter	10926
Syslog Filter	10863
IPFIX Filter	0
E-mail Filter	2
Priority	0
Syslog Event Rate	0
Syslog Data Rate	0

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

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.

Reset Event Count (**X** icon) resets the event counter for an event, a group, or a category, and the event counters of higher levels are recalculated. To reset all counters, use **Reset Event Count** above the table on the **Log Settings > Base Setup** page, as described in Reset Event Count Button.

Configuring Event Attributes Globally

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

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

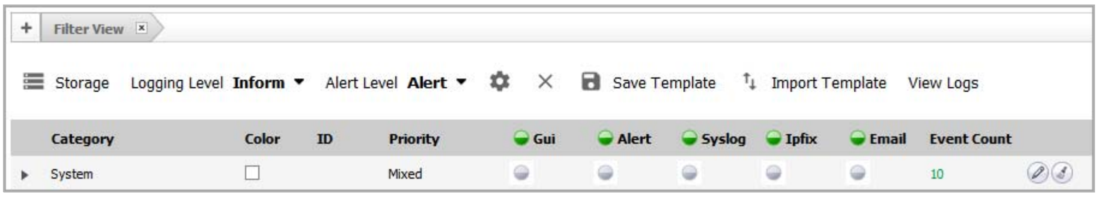
These global attributes can be modified:

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

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

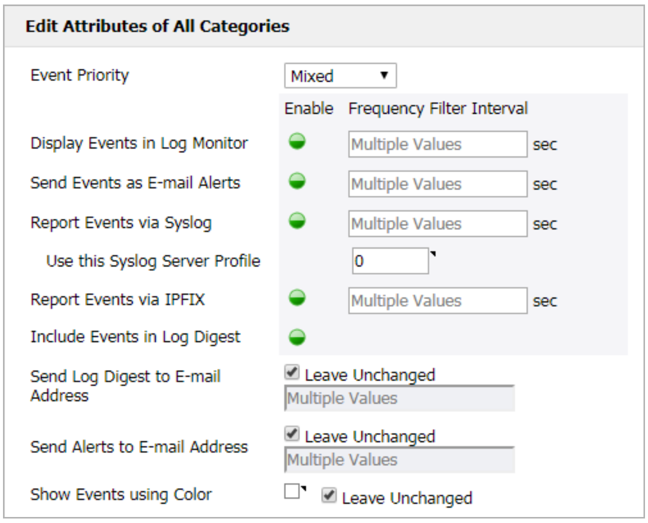
To edit the Category attributes globally:

1 Navigate to the **Logs & Reporting | Log Settings** > **Base Setup** page.



Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count
System	□		Mixed	●	●	●	●	●	10

2 Click the **Configure** icon. The **Edit Attributes of All Categories** pop-up dialog appears.



Edit Attributes of All Categories

Event Priority	Mixed ▾	
	Enable	Frequency Filter Interval
Display Events in Log Monitor	●	Multiple Values sec
Send Events as E-mail Alerts	●	Multiple Values sec
Report Events via Syslog	●	Multiple Values sec
Use this Syslog Server Profile		0
Report Events via IPFIX	●	Multiple Values sec
Include Events in Log Digest	●	
Send Log Digest to E-mail Address	☑ Leave Unchanged Multiple Values	
Send Alerts to E-mail Address	☑ Leave Unchanged Multiple Values	
Show Events using Color	□ ☑ Leave Unchanged	

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

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

When the fields 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.

CAUTION: The changes are saved and overwrite individual settings. Normally, production environments would not set all Categories/Groups/Events to have exactly the same settings. Before doing this, be sure to save your current configuration using the Save Template option, so that the previous settings can be restored if a mistake is made by using Import Template > Custom. Also, factory default settings can be restored using Import Template > Default.

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

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

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

TIP: The different options are independent of each other, and you can enable any combination of them and set different frequencies of generation for them. For example, you might want an event message emailed to you, but it is not shown in the **INVESTIGATE | Logs > Event Logs** page.

When GMS is enabled, however, care must be taken when modifying event attributes so events used to generate reports are not incorrectly filtered out. Explicit modification of individual events are saved even if used for GMS. Before making any changes, save current Log settings using **Save Template**. This way, should a mistake be made, the previous settings can be restored using **Import Template > Custom**. As a last resort, the GMS settings can be restored using **Import Template > Analyzer/Viewpoint/GMS**.

4 If you want to display the log events in the **INVESTIGATE | Logs > Event Logs** page, select the **Enable** icon for the **Display Events in Log Monitor** option.

  a In the **Frequency Filter Interval** field for **Display Events in Log Monitor**, enter the number of seconds that should elapse before allowing the same event to be logged and displayed again when that event occurs one after the other. The range is 0 to 86400.

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

5 If you want to send events as **E-mail Alerts**, select the **Enable** icon for the **Send Events as E-mail Alerts** option.

   a In the **Frequency Filter Interval** field for **Send Events as E-mail Alerts**, enter the number of seconds that should elapse before allowing the same email event to be sent when that event occurs one after the other. The range is 0 to 86400.

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

6 If you want to report events through Syslog, select the **Enable** icon for the **Report Events via Syslog** option.

   a In the **Frequency Filter Interval** field for **Report Events via Syslog**, enter the number of seconds that should elapse before allowing the same Syslog messages to be sent when that event occurs one after the other. The range is 0 to 86400.

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

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

8 If you want to report events through IPFIX, select the **Enable** icon for the **Report Events via IPFIX** option.

   a In the **Frequency Filter Interval** field for **Report Events via IPFIX**, enter the number of seconds that should elapse before allowing the same events to be reported through IPFIX when events occur one after the other. The range is 0 to 86400.

   For example, if you set this value to 60 seconds, then when an event reported through IPFIX first happens at 1:15 p.m., the next report for the same event is not sent until 60 seconds after the first one. Reports to IPFIX for the same event occurring within the 60-second interval are not sent.

9 If you want to include the events in the Log Digest, select the **Enable** icon for the **Include Events in Log Digest** option. The Log Digest is a chronological collation of events.

10 If you enabled **Include Events in Log Digest**, do one of the following for **Send Log Digest to E-mail Address**:

   - If you want to use the same email address that is entered in the **Log Settings > Automation** page even when you change other values in this dialog, select **Leave Unchanged**. This option is enabled by default.

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

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

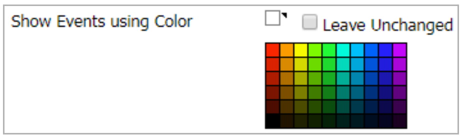
   TIP: An email alert is one email sent for each event occurrence as soon as that event has occurred. A Log Digest, on the other hand, is a chronological collation of events sent as a single email in digest format. Because it is a summation of events, the event information time period is a mix of older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

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

   - If you want to use the same email address that is entered in the **Log Settings > Automation** page even when you change other values in this dialog, select **Leave Unchanged**. This option is enabled by default.

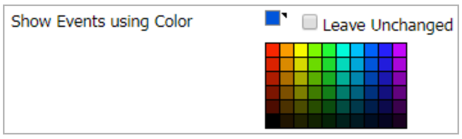
- To change the email address, clear the **Leave Unchanged** option and enter a new address in the now-active field.

12 If you want to use a specific color for all events in all categories, clear the default **Leave Unchanged** option. The color selection matrix appears.



Show Events using Color □ ☐ Leave Unchanged

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



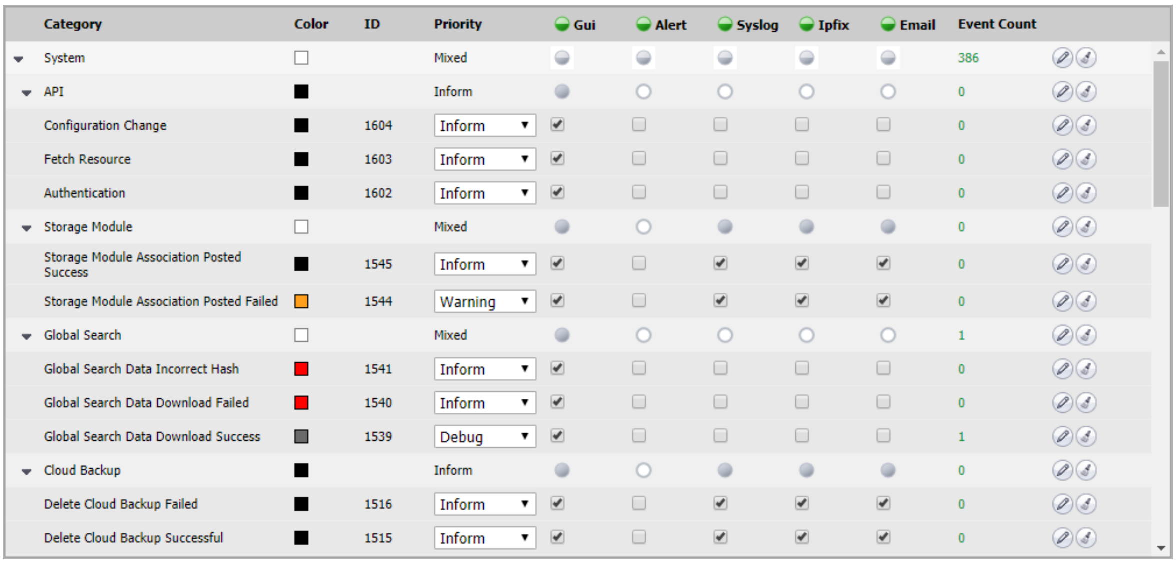
Show Events using Color 🟦 ☐ Leave Unchanged

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 per event.



Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count
System	□		Mixed	◒	◒	◒	◒	◒	386
API	■		Inform	●	○	○	○	○	0
Configuration Change	■	1604	Inform ▾	☑	☐	☐	☐	☐	0
Fetch Resource	■	1603	Inform ▾	☑	☐	☐	☐	☐	0
Authentication	■	1602	Inform ▾	☑	☐	☐	☐	☐	0
Storage Module	□		Mixed	●	○	●	●	●	0
Storage Module Association Posted Success	■	1545	Inform ▾	☑	☐	☑	☑	☑	0
Storage Module Association Posted Failed	🟧	1544	Warning ▾	☑	☐	☑	☑	☑	0
Global Search	□		Mixed	●	○	○	○	○	1
Global Search Data Incorrect Hash	🟥	1541	Inform ▾	☑	☐	☐	☐	☐	0
Global Search Data Download Failed	🟥	1540	Inform ▾	☑	☐	☐	☐	☐	0
Global Search Data Download Success	▨	1539	Debug ▾	☑	☐	☐	☐	☐	1
Cloud Backup	■		Inform	●	○	●	●	●	0
Delete Cloud Backup Failed	■	1516	Inform ▾	☑	☐	☑	☑	☑	0
Delete Cloud Backup Successful	■	1515	Inform ▾	☑	☐	☑	☑	☑	0

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

- **Edit Log Category** dialog modifies settings for a category and all groups that belong to the same category and, consequently, all events in that category.
- **Edit Log Group** dialog modifies settings for a group and all events that belong to that group.
- **Edit Log Event** dialog modifies settings for one specific event.

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

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

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

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

Topics:

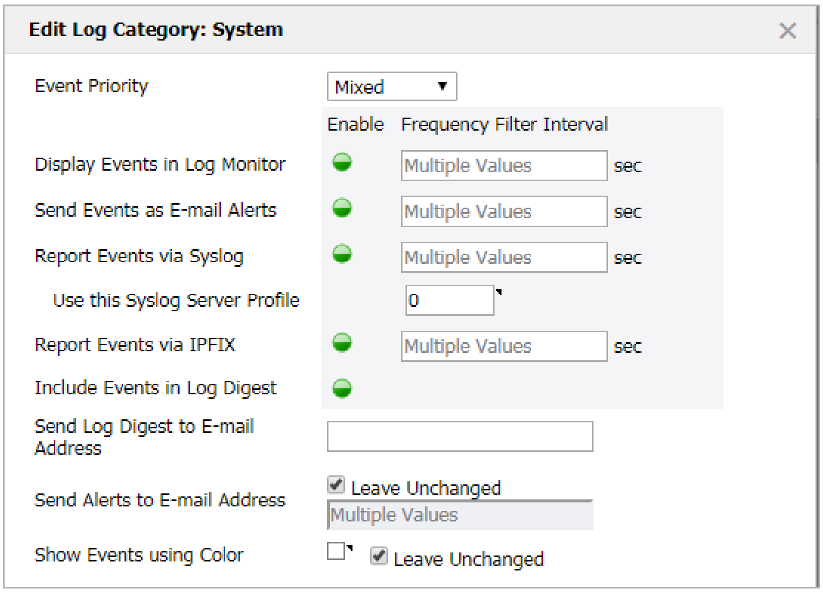
- Configuring Event Attributes by Category
- Configuring Event Attributes by Group
- Configuring Event Attributes by Event
- About Filename Logging

Configuring Event Attributes by Category

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

To set the Event Attributes by category level:

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



Edit Log Category: System

	Enable	Frequency Filter Interval
Event Priority	Mixed ▼	
Display Events in Log Monitor	◓	Multiple Values sec
Send Events as E-mail Alerts	◓	Multiple Values sec
Report Events via Syslog	◓	Multiple Values sec
Use this Syslog Server Profile		0
Report Events via IPFIX	◓	Multiple Values sec
Include Events in Log Digest	◓	
Send Log Digest to E-mail Address		
Send Alerts to E-mail Address	☑ Leave Unchanged Multiple Values	
Show Events using Color	☐ ☑ Leave Unchanged	

2 Follow the steps in Configuring Event Attributes Globally.

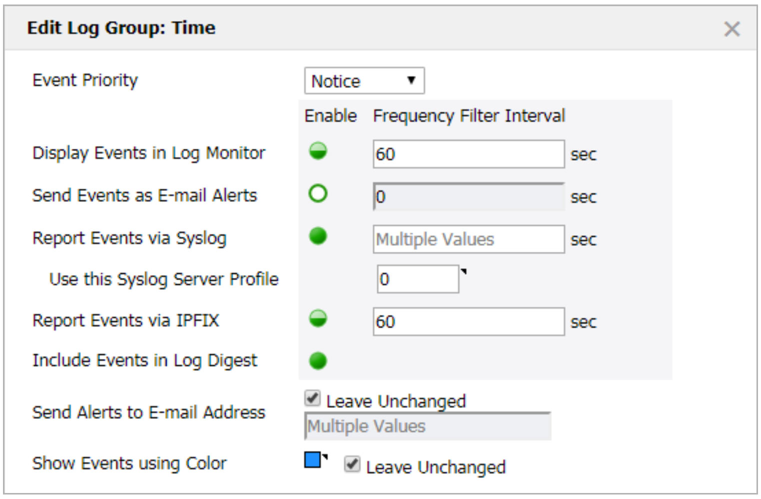
Configuring Event Attributes by Group

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

To set the Event Attributes by group level:

1 In **Log Settings > Base Setup**, click the arrow on the left to expand the category that contains the group you want to edit.

2 Click the **Edit** icon in the right-most column of the row with the group you want to edit. The **Edit Log Group** dialog for that group is displayed.



Edit Log Group: Time

Event Priority	Notice		
	Enable	Frequency Filter Interval	
Display Events in Log Monitor	◐	60	sec
Send Events as E-mail Alerts	○	0	sec
Report Events via Syslog	●	Multiple Values	sec
Use this Syslog Server Profile		0	
Report Events via IPFIX	◐	60	sec
Include Events in Log Digest	●		
Send Alerts to E-mail Address	☑ Leave Unchanged Multiple Values		
Show Events using Color	🟦 ☑ Leave Unchanged		

3 Follow the steps in Configuring Event Attributes Globally.

Configuring Event Attributes by Event

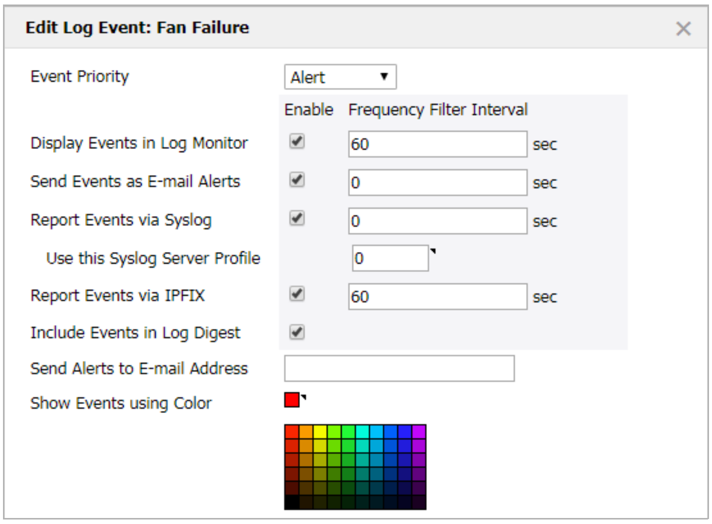
The most granular level, the event level, allows the Event Attributes columns to be directly modified by expanding the selected category into groups, then expanding the selected group into individual events within that group. Any changes done to the event apply to just that event within the selected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

To set the Event Attributes by event level:

1 In **Log Settings > Base Setup**, click the arrow on the left to expand the category that contains the group with the event you want to edit.

2 Click the arrow on the left to expand the group that contains the event you want to edit.

3 Click the **Edit** icon in the right-most column of the row with the event you want to edit. The **Edit Log Event** dialog for that event is displayed.



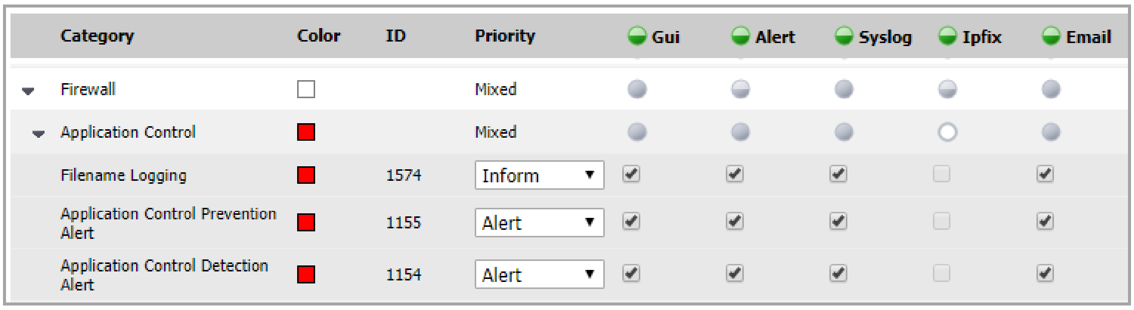
Edit Log Event: Fan Failure

Event Priority	Alert ▾		
	Enable	Frequency Filter Interval	
Display Events in Log Monitor	☑	60	sec
Send Events as E-mail Alerts	☑	0	sec
Report Events via Syslog	☑	0	sec
Use this Syslog Server Profile		0	
Report Events via IPFIX	☑	60	sec
Include Events in Log Digest	☑		
Send Alerts to E-mail Address			
Show Events using Color	🟥		

4 Follow the steps in Configuring Event Attributes Globally.

About Filename Logging

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



Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email
Firewall	□		Mixed	●	●	●	●	●
Application Control	🟥		Mixed	●	●	●	○	●
Filename Logging	🟥	1574	Inform ▾	☑	☑	☑	□	☑
Application Control Prevention Alert	🟥	1155	Alert ▾	☑	☑	☑	□	☑
Application Control Detection Alert	🟥	1154	Alert ▾	☑	☑	☑	□	☑

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

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

- **Enable App Control**

  Application Control is enabled per zone from the **Network > Zones** page and globally on **MANAGE | Policies | Rules > App Control**.

- **Enable Filename Logging**

  Filename Logging is enabled on **MANAGE | Logs & Reporting | Log Settings > Base Setup**.

- **Logging is enabled for the App Control Filename Logging event id=1574**

  Enable **GUI** or **Syslog** with appropriate filtering on **MANAGE | Logs & Reporting | Log Settings > Base Setup**.

Filename Logging works with the following protocols:

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

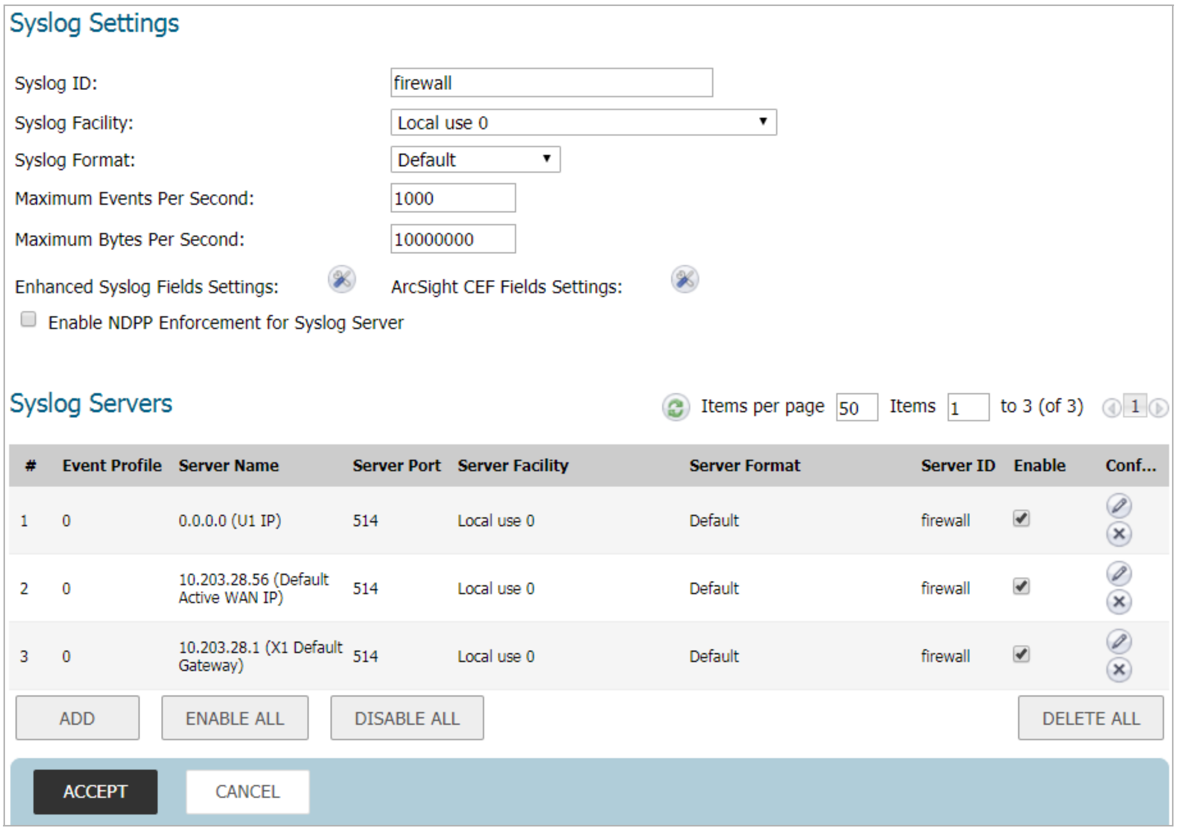
Gateway Anti-Virus does not need to be enabled.

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

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

4

Configuring Syslog Settings



Syslog Settings

Syslog ID:	firewall
Syslog Facility:	Local use 0
Syslog Format:	Default
Maximum Events Per Second:	1000
Maximum Bytes Per Second:	10000000

Enhanced Syslog Fields Settings: ArcSight CEF Fields Settings:

□ Enable NDPP Enforcement for Syslog Server

Syslog Servers

Items per page 50 Items 1 to 3 (of 3)

#	Event Profile	Server Name	Server Port	Server Facility	Server Format	Server ID	Enable	Conf...
1	0	0.0.0.0 (U1 IP)	514	Local use 0	Default	firewall	☑	
2	0	10.203.28.56 (Default Active WAN IP)	514	Local use 0	Default	firewall	☑	
3	0	10.203.28.1 (X1 Default Gateway)	514	Local use 0	Default	firewall	☑	

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

ⓘ **NOTE:** See *RCF 3164 - The BSD Syslog Protocol* for more information.

ⓘ **NOTE:** Syslog output might 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 on page 63.

ⓘ **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.

Packet data can be sent to Syslog Servers. For information on 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

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

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

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

About Syslog Server Profiling

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

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

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

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

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

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

Using a GMS Server for Syslog

GMS can be enabled or disabled only on the **MANAGE | System Settings | Appliance > Base Settings** page under **Advanced Management** (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 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 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. 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.

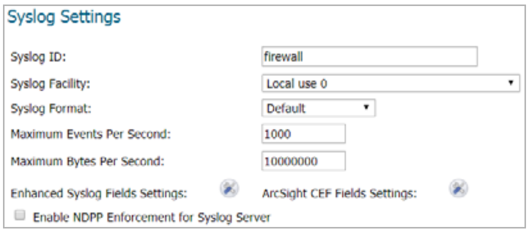
Syslog Settings

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**. Therefore, these fields are grayed-out and cannot be modified. All other fields, however, can still be customized as needed.

To configure Syslog settings on your firewall:

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



Syslog Settings

Syslog ID: firewall

Syslog Facility: Local use 0

Syslog Format: Default

Maximum Events Per Second: 1000

Maximum Bytes Per Second: 10000000

Enhanced Syslog Fields Settings:

ArcSight CEF Fields Settings:

☐ Enable NDPP Enforcement for Syslog Server

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=`. Therefore, for the default value, `firewall`, all Syslog messages include `id=firewall`. The ID can be set to a string consisting of 0 to 32 alphanumeric and underscore characters.

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

Syslog Facility

Kernel

User-Level Messages

UUCP Subsystem

Clock Daemon (BSP Linux)

Local Use 0 [1]

Local Use 1

Syslog Facility (Continued)

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 **Limiting Saved Records** - You can limit the maximum number of events logged to prevent the internal or external logging mechanism from being overwhelmed by logged events. **Enable Data Rate Limiting** is used to accomplish this action.

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

Specify the maximum number of bytes in the Maximum Bytes Per Second field. The default minimum is 0, and the maximum is 1,000,000,000. The default maximum is 10,000,000 bytes per second.

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

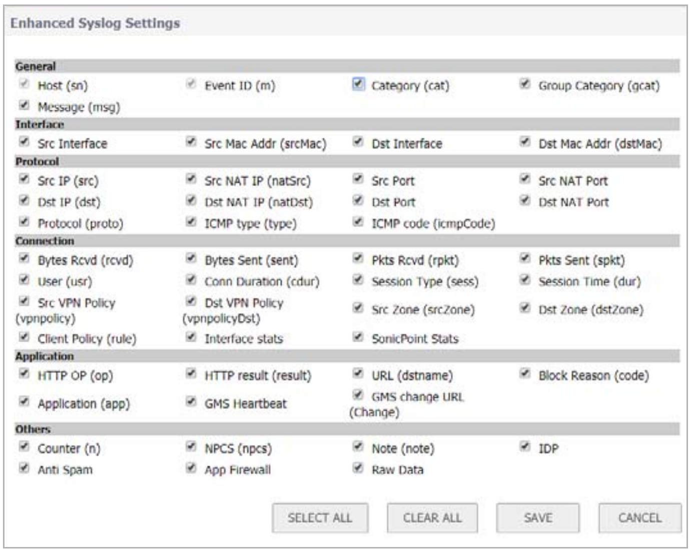
Syslog Formats

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 If you selected:

- **Default** or **WebTrends**, go to Step 14.
- **Enhanced Syslog**, go to Step 7.
- **ArcSight**, go to Step 11.

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



Enhanced Syslog Settings

General

☑ Host (sn) ☑ Event ID (m) ☑ Category (cat) ☑ Group Category (gcat)
☑ Message (msg)

Interface

☑ Src Interface ☑ Src Mac Addr (srcMac) ☑ Dst Interface ☑ Dst Mac Addr (dstMac)

Protocol

☑ Src IP (src) ☑ Src NAT IP (natSrc) ☑ Src Port ☑ Src NAT Port
☑ Dst IP (dst) ☑ Dst NAT IP (natDst) ☑ Dst Port ☑ Dst NAT Port
☑ Protocol (proto) ☑ ICMP type (type) ☑ ICMP code (icmpCode)

Connection

☑ Bytes Rcvd (rcvd) ☑ Bytes Sent (sent) ☑ Pkts Rcvd (rpkt) ☑ Pkts Sent (spkt)
☑ User (usr) ☑ Conn Duration (cdur) ☑ Session Type (sess) ☑ Session Time (dur)
☑ Src VPN Policy (vpnpolicy) ☑ Dst VPN Policy (vpnpolicyDst) ☑ Src Zone (srcZone) ☑ Dst Zone (dstZone)
☑ Client Policy (rule) ☑ Interface stats ☑ SonicPoint Stats

Application

☑ HTTP OP (op) ☑ HTTP result (result) ☑ URL (dstname) ☑ Block Reason (code)
☑ Application (app) ☑ GMS Heartbeat ☑ GMS change URL (Change)

Others

☑ Counter (n) ☑ NPCS (npcs) ☑ Note (note) ☑ IDP
☑ Anti Spam ☑ App Firewall ☑ Raw Data

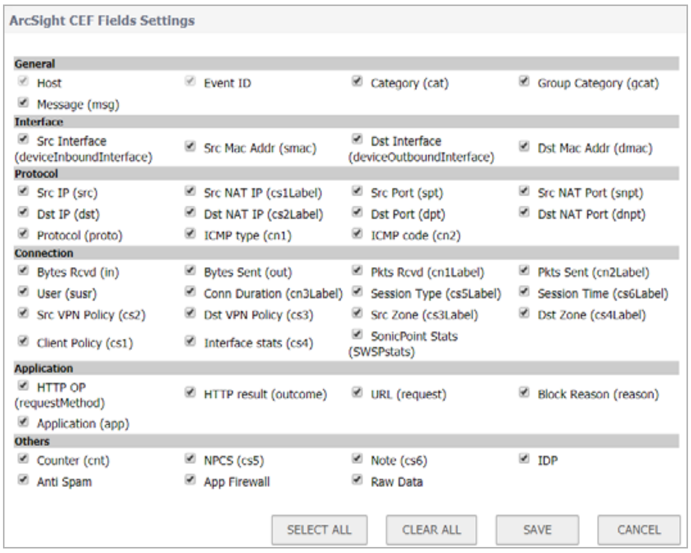
8 (Optional) Select the **Enhanced Syslog** options to log. By default, all options are selected; the **Host (sn)** and **Event ID (m)** options are dimmed as they cannot be changed. To:

- 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.

9 Click **Save**.

10 Go to Step 14.

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



ArcSight CEF Fields Settings

General

☑ Host ☑ Event ID ☑ Category (cat) ☑ Group Category (gcat)
☑ Message (msg)

Interface

☑ Src Interface (deviceInboundInterface) ☑ Src Mac Addr (smac) ☑ Dst Interface (deviceOutboundInterface) ☑ Dst Mac Addr (dmac)

Protocol

☑ Src IP (src) ☑ Src NAT IP (cs1Label) ☑ Src Port (spt) ☑ Src NAT Port (snpt)
☑ Dst IP (dst) ☑ Dst NAT IP (cs2Label) ☑ Dst Port (dpt) ☑ Dst NAT Port (dnpt)
☑ Protocol (proto) ☑ ICMP type (cn1) ☑ ICMP code (cn2)

Connection

☑ Bytes Rcvd (in) ☑ Bytes Sent (out) ☑ Pkts Rcvd (cn1Label) ☑ Pkts Sent (cn2Label)
☑ User (susr) ☑ Conn Duration (cn3Label) ☑ Session Type (cs5Label) ☑ Session Time (cs6Label)
☑ Src VPN Policy (cs2) ☑ Dst VPN Policy (cs3) ☑ Src Zone (cs3Label) ☑ Dst Zone (cs4Label)
☑ Client Policy (cs1) ☑ Interface stats (cs4) ☑ SonicPoint Stats (SWSPstats)

Application

☑ HTTP OP (requestMethod) ☑ HTTP result (outcome) ☑ URL (request) ☑ Block Reason (reason)
☑ Application (app)

Others

☑ Counter (cnt) ☑ NPCS (cs5) ☑ Note (cs6) ☑ IDP
☑ Anti Spam ☑ App Firewall ☑ Raw Data

12 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.

13 Click **Save**.

14 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.

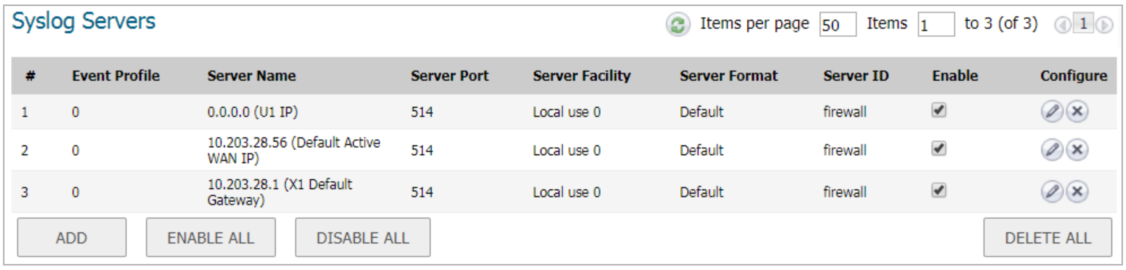
15 Optionally, specify the maximum number of bytes in the **Maximum Bytes Per Second** field; the minimum is number is 0 bytes per second, the maximum is 1000000000 bytes per second, and the default is **10000000**. This control limits data logged to prevent the internal or external logging mechanism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

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

16 Optionally, select the **Enable NDPP Enforcement for Syslog Server**.

17 Click **Accept**.

Syslog Servers



Syslog Servers

Items per page 50 Items 1 to 3 (of 3) 1

#	Event Profile	Server Name	Server Port	Server Facility	Server Format	Server ID	Enable	Configure
1	0	0.0.0.0 (U1 IP)	514	Local use 0	Default	firewall	☑	
2	0	10.203.28.56 (Default Active WAN IP)	514	Local use 0	Default	firewall	☑	
3	0	10.203.28.1 (X1 Default Gateway)	514	Local use 0	Default	firewall	☑	

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.

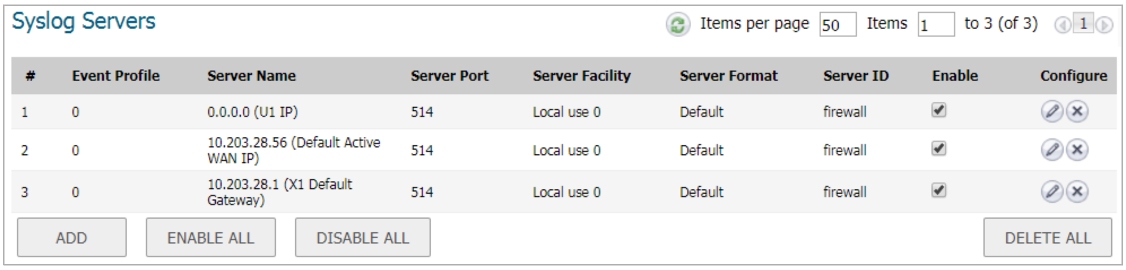
Global settings affect all servers. For example, a change in a global format changes the format of all the servers to the selected value.

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.

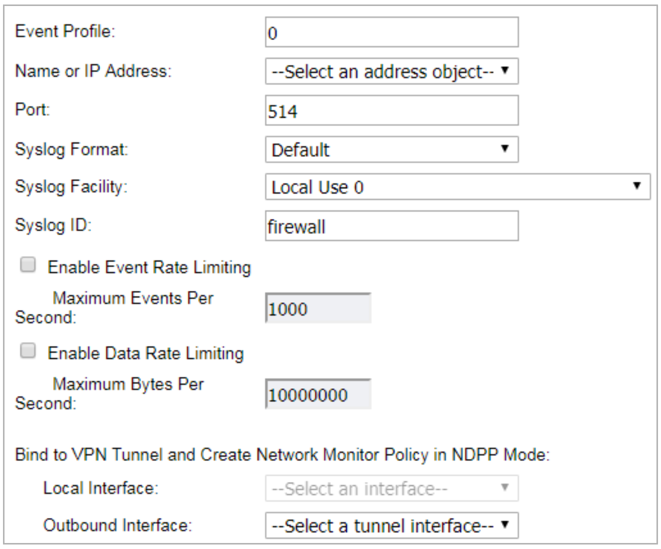


Syslog Servers

Items per page 50 Items 1 to 3 (of 3)

#	Event Profile	Server Name	Server Port	Server Facility	Server Format	Server ID	Enable	Configure
1	0	0.0.0.0 (U1 IP)	514	Local use 0	Default	firewall	☑	
2	0	10.203.28.56 (Default Active WAN IP)	514	Local use 0	Default	firewall	☑	
3	0	10.203.28.1 (X1 Default Gateway)	514	Local use 0	Default	firewall	☑	

3 Click **Add**. The **Add Syslog Server** dialog appears.



Event Profile:	0
Name or IP Address:	--Select an address object--
Port:	514
Syslog Format:	Default
Syslog Facility:	Local Use 0
Syslog ID:	firewall
□ Enable Event Rate Limiting	
Maximum Events Per Second:	1000
□ Enable Data Rate Limiting	
Maximum Bytes Per Second:	10000000

Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode:

Local Interface:	--Select an interface--
Outbound Interface:	--Select a tunnel interface--

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 therefore, prevent the internal or external logging mechanism from being overwhelmed by log events, select **Enable Event Rate Limiting**.

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

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.

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

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

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 t**h**e 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.

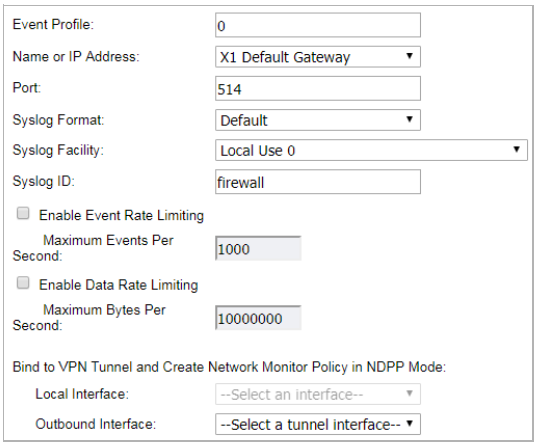
b Optionally, choose an Interface from the **Outbound Interface** drop-down menu.

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.



Event Profile: 0

Name or IP Address: X1 Default Gateway ▾

Port: 514

Syslog Format: Default ▾

Syslog Facility: Local Use 0 ▾

Syslog ID: firewall

□ Enable Event Rate Limiting

Maximum Events Per Second: 1000

□ Enable Data Rate Limiting

Maximum Bytes Per Second: 10000000

Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode:

Local Interface: --Select an interface-- ▾

Outbound Interface: --Select a tunnel interface-- ▾

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

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 **Enable All**.

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 **Disable All**.

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.

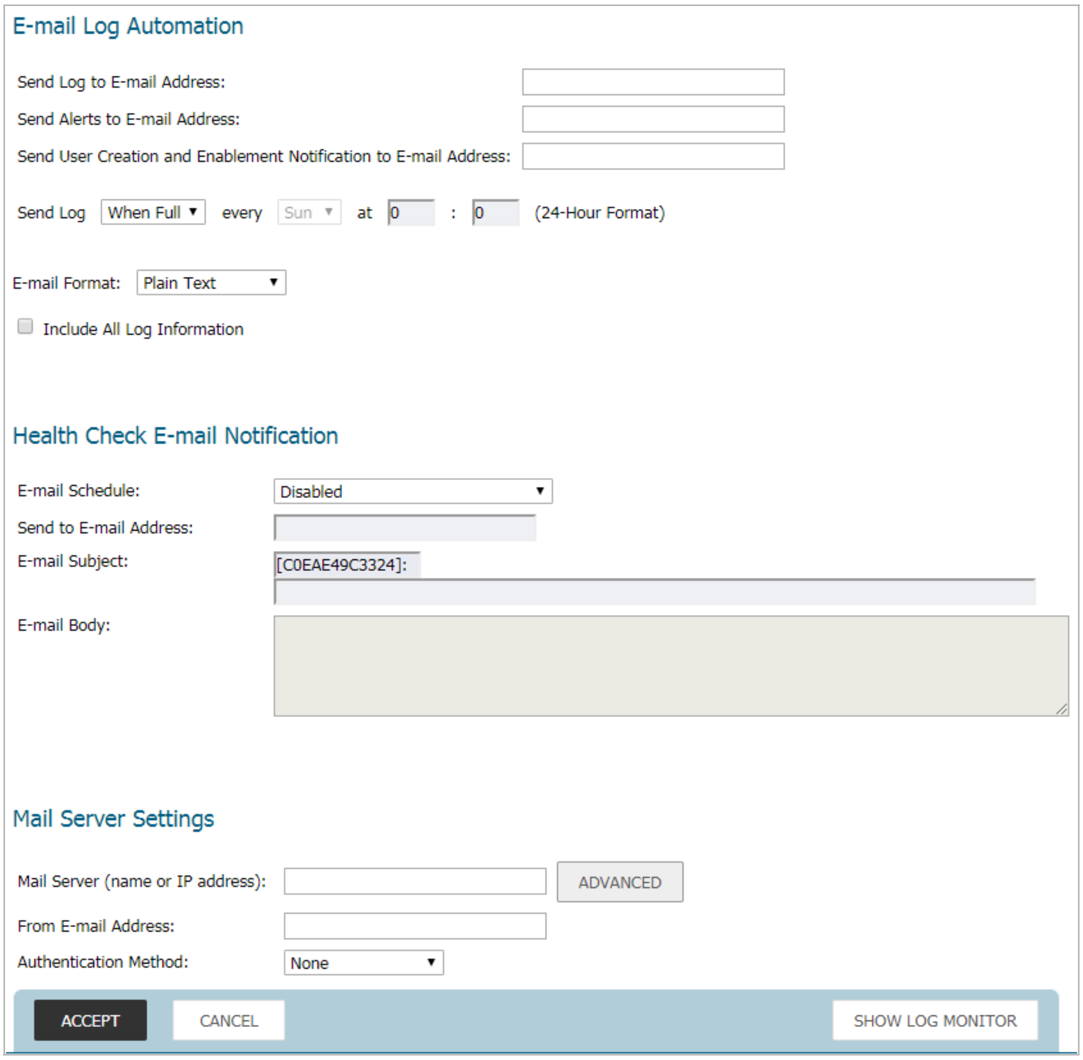
To delete all Syslog Servers:

1 Click **Disable All**.

5

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.



E-mail Log Automation

Send Log to E-mail Address:

Send Alerts to E-mail Address:

Send User Creation and Enablement Notification to E-mail Address:

Send Log When Full every Sun at 0 : 0 (24-Hour Format)

E-mail Format: Plain Text

□ Include All Log Information

Health Check E-mail Notification

E-mail Schedule: Disabled

Send to E-mail Address:

E-mail Subject: [C0EAE49C3324]:

E-mail Body:

Mail Server Settings

Mail Server (name or IP address):

From E-mail Address:

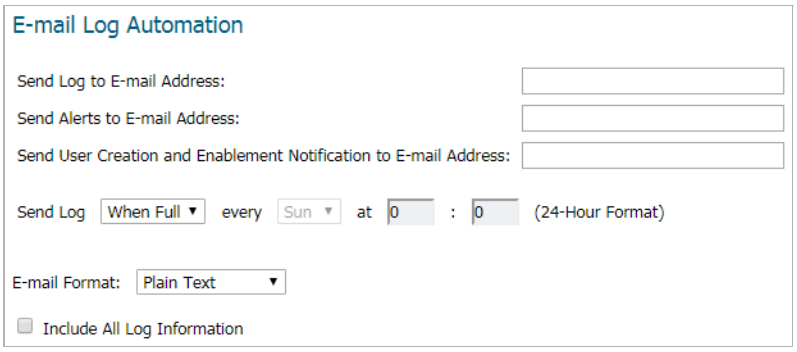
Authentication Method: None

Topics:

- Email Log Automation
- Health Check Email Notification
- Mail Server Settings
- FTP Log Automation
- Solera Capture Stack

Email Log Automation

The next sections describe the procedure for automating email dispatching. You can also send an email of logs manually at any time. For a description of this procedure, see: Manually Emailing Auditing Records.



E-mail Log Automation

Send Log to E-mail Address:

Send Alerts to E-mail Address:

Send User Creation and Enablement Notification to E-mail Address:

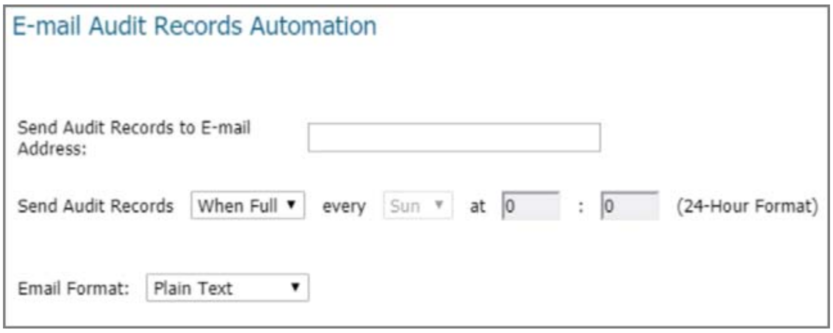
Send Log When Full every Sun at 0 : 0 (24-Hour Format)

E-mail Format: Plain Text

□ Include All Log Information

- **Send Log to Email address** - To receive the Log Digest through email, enter your email address (`username@mydomain.com`). After being sent, the Log Digest is cleared from the SonicWall memory. If this field is left blank, the Log Digest is not emailed.
- **Send Alerts to Email address** - To be emailed immediately when attacks or system errors occur, enter your email address (`username@mydomain.com`) as a standard email address or an email paging service. If this field is left blank, email alert messages are not sent.
- **Send User Creation and Enablement Notification to Email Address** – To be emailed immediately when a user has been created and enabled, enter your email address (`username@mydomain.com`). If this field is left blank, email notifications are not sent.
- **Send Log** - Determines the frequency of sending Log Digest files. The options in the drop-down menu are:
  - **When Full** - This setting is the default.
  - **Weekly** - Select the day of the week the Log Digest is sent in 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 Digest is to be sent in 24-hour format in the **At** field.
- **Email Format** - Select whether log emails are sent in **Plain Text** or **HTML** format or as a **CSV Attachment** from the drop-down menu.
- **Include All Log Information** - Select to have all information included in the log report. If not selected, only readable column data is sent.
- If finished configuring settings on this page, click **ACCEPT**.

Email Audit Records Automation



E-mail Audit Records Automation

Send Audit Records to E-mail Address:

Send Audit Records When Full ▾ every Sun ▾ at 0 : 0 (24-Hour Format)

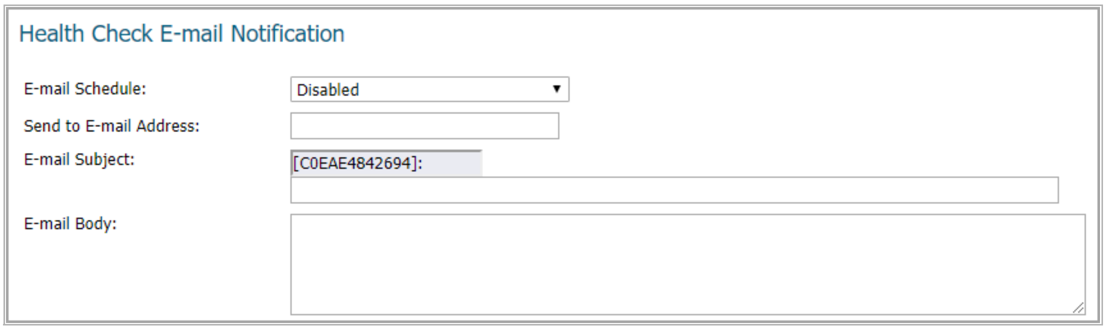
Email Format: Plain Text ▾

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

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

Health Check Email Notification

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



Health Check E-mail Notification

E-mail Schedule: Disabled

Send to E-mail Address:

E-mail Subject: [C0EAE4842694]:

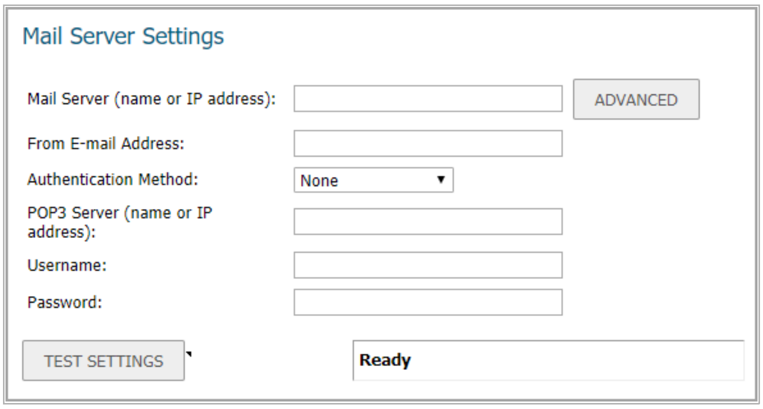
E-mail Body:

To set up a Health Check Email Notification:

1. From the **Email Schedule** drop-down menu, select a predefined schedule, **Create a new schedule**, or **Disabled**.
2. In the **Send to Email Address** field, enter the email address of the recipient(s) to notify.
3. In the **E-mail Subject** field, enter the subject of the email. The **Firewall Name** is included by default. The **Firewall Name** is configured on **MANAGE | System Setup | Appliance > Base Settings**, and is the appliance serial number by default.
4. In the **Email Body** field, enter the body of email.
5. If finished configuring settings on this page, click **ACCEPT**.

Mail Server Settings

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



Mail Server Settings

Mail Server (name or IP address):

From E-mail Address:

Authentication Method: None

POP3 Server (name or IP address):

Username:

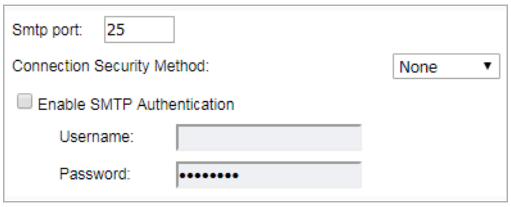
Password:

Ready

- **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: 25

Connection Security Method: None

□ Enable SMTP Authentication

Username:

Password: ••••••••

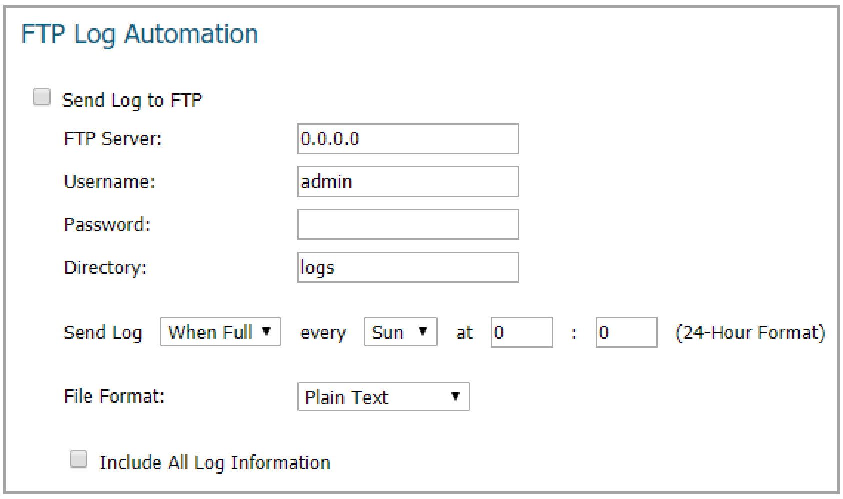
  - **Smtp port** - Enter the SMTP port used for email. The default port number is 25.
  - **Connection Security Method** - Select a security method for the email from the drop-down menu:
    - **None** (default)
    - **SSL**/TLS
    - **STARTTLS**
  - **Enable SMTP Authentication** - Select to enable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

FTP Log Automation

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

- You can select text, HTML, or CSV file format
- You can select detailed or concise log information

- You can select a predefined time schedule. In addition to the defined schedule, logs are sent when the administrator clicks **restart** and when the log is full.



FTP Log Automation

□ Send Log to FTP

FTP Server: 0.0.0.0

Username: admin

Password:

Directory: logs

Send Log When Full ▼ every Sun ▼ at 0 : 0 (24-Hour Format)

File Format: Plain Text ▼

□ Include All Log Information

To configure FTP log automation settings:

1 Navigate to the **MANAGE | Logs & Reporting | Log Settings > Automation** page and scroll down to the **FTP Log Automation** section.

2 Select **Send Log to FTP** to enable FTP log automation. Clear the checkbox to disable it.

3 For **FTP Server**, enter the IPv4 address of the FTP server.

4 For **Username**, enter the username for authenticating to the FTP server.

5 For **Password**, enter the password for the FTP server account.

6 For **Directory**, enter the destination directory on the FTP server. The default is **logs**.

7 From the **Send Log** drop-down menu, select the frequency for sending the logs to the FTP server. Choose **Daily**, **Weekly**, or **When Full**. The default is **When Full**.

8 Select the day of the week for sending the logs from the drop-down menu next to **every**. This is used for a Weekly schedule.

9 Select the hour and minute of the day in 24 hour format in the two fields next to **(24-Hour Format)**. The time is used for Daily and Weekly schedules.

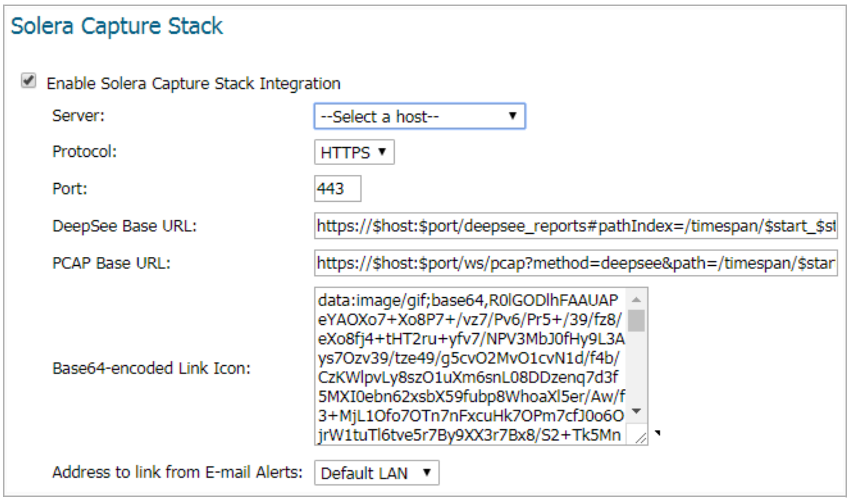
10 From the **File Format** drop-down menu, select one of **Plain Text**, **HTML**, or **CSV Attachment** as the format in which the logs are sent.

11 Select **Include All Log Information** to have all information included in the log report. If not selected, only readable column data is sent.

12 If finished configuring settings on this page, click **ACCEPT**.

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 completed on a live network through NPCS while the device is actively capturing and archiving data.



Solera Capture Stack

☑ Enable Solera Capture Stack Integration

Server:	--Select a host--
Protocol:	HTTPS
Port:	443
DeepSee Base URL:	https://$host:$port/deepsee_reports#pathIndex=/timespan/$start_$st
PCAP Base URL:	https://$host:$port/ws/pcap?method=deepsee&path=/timespan/$star
Base64-encoded Link Icon:	data:image/gif;base64,R0lGODlhFAAUAP eYAOXo7+Xo8P7+/vz7/Pv6/Pr5+/39/fz8/ eXo8fj4+tHT2ru+yfv7/NPV3MbJ0fHy9L3A ys7Ozv39/tze49/g5cvO2MvO1cvN1d/f4b/ CzKWlpvLy8szO1uXm6snL08DDzenq7d3f 5MXI0ebn62xsbX59fubp8WhoaXl5er/Aw/f 3+MjL1Ofo7OTn7nFxcuHk7OPm7cfJ0o6O jrW1tuTl6tve5r7By9XX3r7Bx8/S2+Tk5Mn
Address to link from E-mail Alerts:	Default LAN

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:

- **$host** - server name or IP address that has the data
- **$port** - HTTP/HTTPS port number where the server is listening
- **$usr** - user name for authentication
- **$pwd** - password for authentication
- **$start** - start date and time
- **$stop** - stop date and time
- **$ipproto** - IP protocol
- **$scrip** - source IP address
- **$dstip** - destination IP address
- **$srcport** - source port
- **$dstport** - destination port

6 If finished configuring settings on this page, click **ACCEPT**.

7 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.

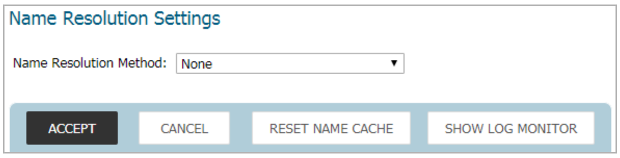
8 In the **Base64-encoded Link Icon** field, define the Base 64-encoded GIF image to be used as desktop shortcut to the Solera server. Ensure the icon is valid and the size is as small as possible. A default icon is given.

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

6

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.



Name Resolution Settings

Name Resolution Method: None

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 does not attempt to resolve IP addresses and Names in the log reports.
- **DNS**: The security appliance uses the DNS server you specify to resolve addresses and names.
- **NetBIOS**: The security appliance uses NetBIOS to resolve addresses and names. If you select NetBIOS, no further configuration is necessary.
- **DNS then NetBIOS**: The security appliance first uses the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it tries again with NetBIOS.

Specifying the DNS Server

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

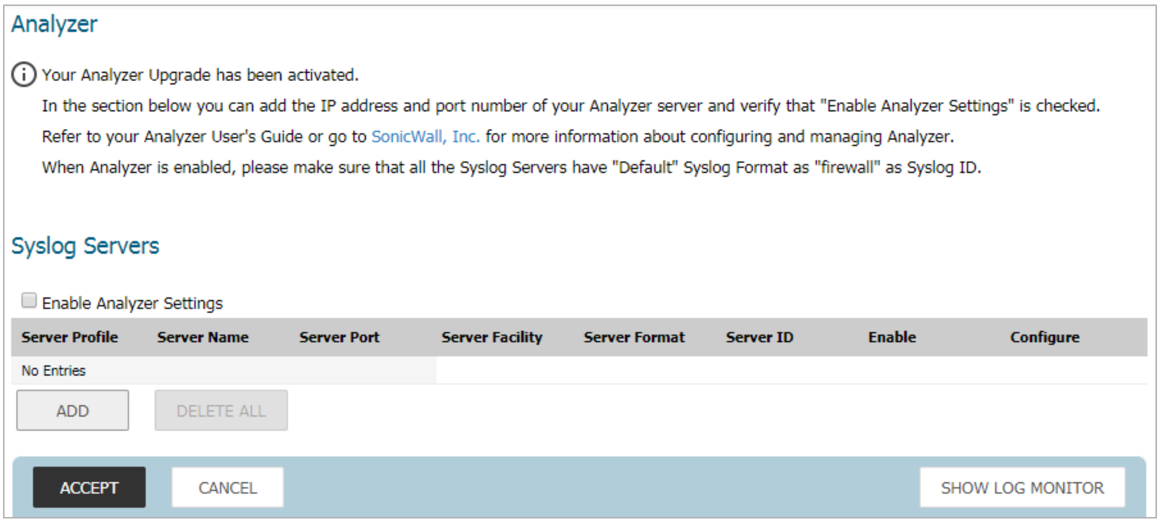
1. Select **Specify DNS Servers Manually** or **Inherit DNS Settings Dynamically from WAN Zone**. The second choice is selected by default.
2. If you selected to specify a DNS server, enter the IP address for at least one DNS server on your network. You can enter up to three servers.
3. Click **Accept**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

7

Configuring the Log Analyzer

NOTE: This feature has been deprecated, starting with SonicOS 6.5.3. The information given here is for reference only.

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



Analyzer

ⓘ Your Analyzer Upgrade has been activated.

In the section below you can add the IP address and port number of your Analyzer server and verify that "Enable Analyzer Settings" is checked.

Refer to your Analyzer User's Guide or go to SonicWall, Inc. for more information about configuring and managing Analyzer.

When Analyzer is enabled, please make sure that all the Syslog Servers have "Default" Syslog Format as "firewall" as Syslog ID.

Syslog Servers

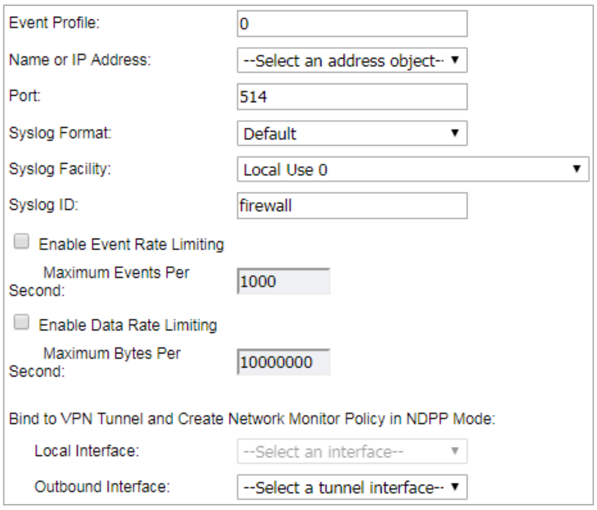
□ Enable Analyzer Settings

Server Profile	Server Name	Server Port	Server Facility	Server Format	Server ID	Enable	Configure
No Entries							

To add an analyzer server connection to your firewall:

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

2 Click **Add**. The **Add Syslog Server** dialog appears.



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

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** can 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 [1]
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

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

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

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

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

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

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

Specify the maximum number of bytes in the **Maximum Bytes Per Second field;** the minimum is number is 0, the maximum is 1000000000, and the default is **10000000** bytes per second.

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**.

8

Configuration Auditing

Topics:

Configuration Auditing Overview

This section describes in detail the recording feature available in SonicOS, versions 6.5.4.5 and higher, that collects and records information on any changes in the security appliance configuration. To access this feature, navigate to **MANAGE | Log Settings > Auditing Records** in the SonicOS web management interface.

Topics:

What is Configuration Auditing

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

Benefits of Configuration Auditing

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

- Automatic documentation of any configuration changes performed by an administrator
- Assistance in troubleshooting unexpected changes in run-time system behavior

- Visibility, continuity, and consistency where there are several administrators, either simultaneously or consecutively. Each administrator has access to a record of changes performed or attempted by all other administrators.
- Third party integration with Firewall Manager, SEIM systems, logging and reporting solutions
- Compliance with regulations such as SOX, FISMA, NIST, DISA STIP

What Information is Recorded

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

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

What Information is Not Recorded

The following are not included in the Configuration Auditing operation:

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

Audit Recording in High Availability Configurations

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

Modifying and Supplementing Configuration Auditing

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

- SNMP Trap Control
- E-CLI Commands

SNMP Trap Control

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

E-CLI Commands

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

- **to work with settings:**

```
config(C0EAE49CE84C)# log audit settings
(config-audit)# enable
(config-audit)# debug
(config-audit)# auditall
(config-audit)# commit
```

- **to show audit records:**

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

Auditing Record Storage and Persistence

Configuration auditing records are saved to non-volatile storage (such as flash), so that records can be restored, if required, after a reboot. The number of records saved is directly proportional to the capability of the device, as defined in the product matrix below. Higher-end platforms can store more records than lower-end devices. Devices with no flash or smaller flash capacity do not support configuration auditing.

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

The maximum number of records that can be stored is defined according to the RAM and flash size of the appliance platform, as given in the table below.

Maximum Number of Records

Firewall models	Flash Memory	Maximum Auditing Records	Auditing Records Persistence Support
NS*a* 9650	64GB RAM, 4 GB Flash	2500	Yes
NS*a* 9450, SuperMassive 9600	16GB RAM, 4 GB Flash	2500	Yes
NS*a* 9250, SuperMassive 9400	16GB RAM, 4 GB Flash	2500	Yes
SuperMassive 9200	8GB RAM, 4 GB Flash	2500	Yes
NS*a* 6650	16GB RAM, 4 GB Flash	2500	Yes
NS*a* 5650, 4650, 3650	8GB RAM, 2GB Flash	2500	Yes
NSA 6600, 5600, NS*a* 2650	4GB RAM, 1GB Flash	2000	Yes
NSA 4600, 3600, 2600	2GB RAM, 1GB Flash	2000	Yes
TZ 350, 350W, 300P	64MB Flash	500	No
TZ 600, 600P, 500, 500W, 400, 400W, 300, 300W	1GB RAM, 64MB Flash	500	No
SOHO 250, SOHO 250W	64MB Flash	500	No
SOHO W	1GB RAM, 64MB Flash	500	No

Managing the Auditing Records Table

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

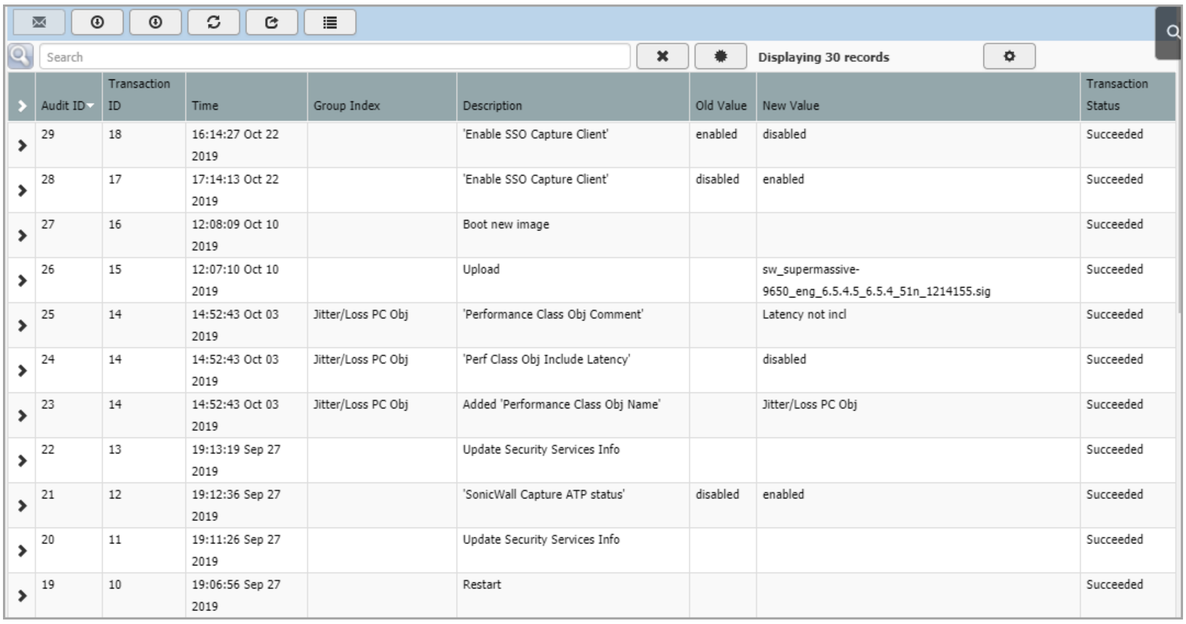
Topics:

- Viewing Auditing Records
- Manually Emailing Auditing Records
- Exporting Auditing Records
- Refreshing the Auditing Records Table
- Displaying the Auditing Records on the Console
- Auditing All Parameters During Addition

Viewing Auditing Records

The **MANAGE | Log Settings > Auditing Records** page displays all the configuration auditing records. It allows a user to view, search, and sort the records.

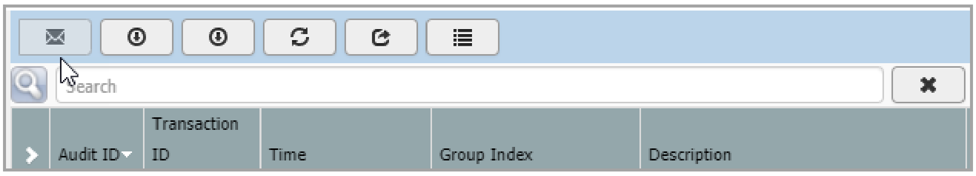
- The user can customize the columns by clicking the **Show**, **Hide** or **Rearrange Columns** button.
- There are also buttons for **Show all Columns** and **Reset to Default** for ease of operation.
- The user can search for a specific string pattern and highlight the matched results, if any are found.
- The first column is expandable to display the summary of the log entry.
- Failed configuration changes are marked in red.
- All columns are sortable.



	Audit ID	Transaction ID	Time	Group Index	Description	Old Value	New Value	Transaction Status
›	29	18	16:14:27 Oct 22 2019		'Enable SSO Capture Client'	enabled	disabled	Succeeded
›	28	17	17:14:13 Oct 22 2019		'Enable SSO Capture Client'	disabled	enabled	Succeeded
›	27	16	12:08:09 Oct 10 2019		Boot new image			Succeeded
›	26	15	12:07:10 Oct 10 2019		Upload		sw_supermassive-9650_eng_6.5.4.5_6.5.4_51n_1214155.sig	Succeeded
›	25	14	14:52:43 Oct 03 2019	Jitter/Loss PC Obj	'Performance Class Obj Comment'		Latency not incl	Succeeded
›	24	14	14:52:43 Oct 03 2019	Jitter/Loss PC Obj	'Perf Class Obj Include Latency'		disabled	Succeeded
›	23	14	14:52:43 Oct 03 2019	Jitter/Loss PC Obj	Added 'Performance Class Obj Name'		Jitter/Loss PC Obj	Succeeded
›	22	13	19:13:19 Sep 27 2019		Update Security Services Info			Succeeded
›	21	12	19:12:36 Sep 27 2019		'SonicWall Capture ATP status'	disabled	enabled	Succeeded
›	20	11	19:11:26 Sep 27 2019		Update Security Services Info			Succeeded
›	19	10	19:06:56 Sep 27 2019		Restart			Succeeded

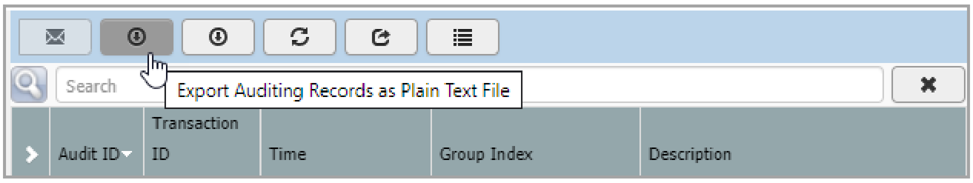
Manually Emailing Auditing Records

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

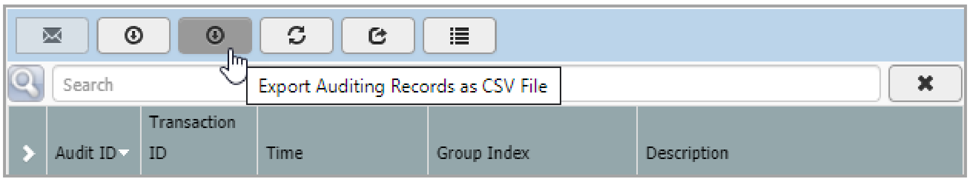


Exporting Auditing Records

There are two export options for auditing records. The button next to the email button on the tool bar is for exporting the records as a text file.

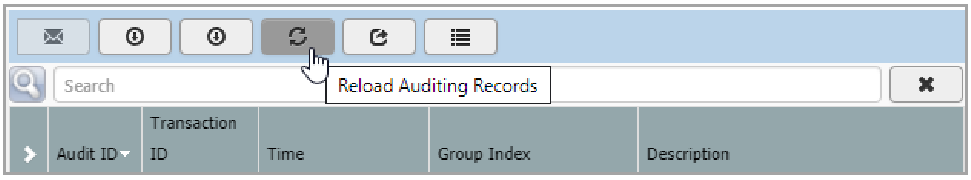


The next button is for exporting the records as a CSV file.



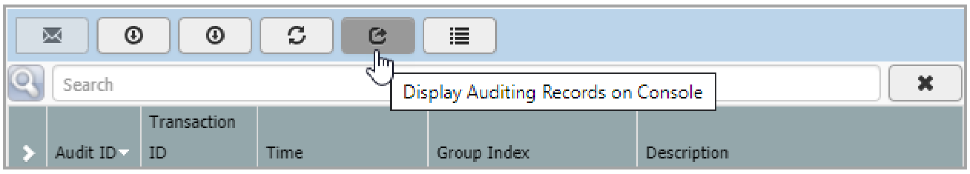
Refreshing the Auditing Records Table

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



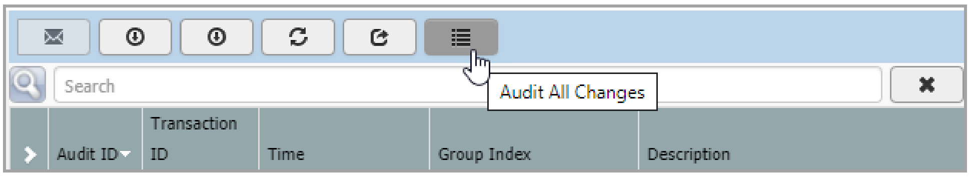
Displaying the Auditing Records on the Console

You can click the **Display Auditing Records on Console** button to display the auditing records on the console in a text format:



Auditing All Parameters During Addition

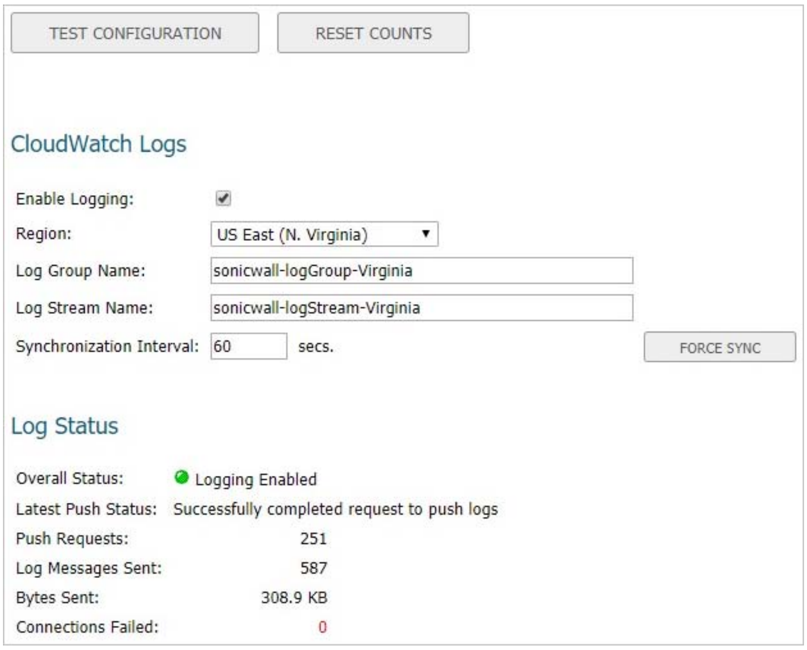
By default, configuration auditing only logs significant changes, defined as changes where the new value of the parameter is different from the default value. You can click the Audit All Changes button to record all parameter changes during an addition activity, even when the new values are the same as the default values.



9

Configuring AWS Logs

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.



CloudWatch Logs

Enable Logging:	☑
Region:	US East (N. Virginia)
Log Group Name:	sonicwall-logGroup-Virginia
Log Stream Name:	sonicwall-logStream-Virginia
Synchronization Interval:	60 secs.

Log Status

Overall Status:	● Logging Enabled
Latest Push Status:	Successfully completed request to push logs
Push Requests:	251
Log Messages Sent:	587
Bytes Sent:	308.9 KB
Connections Failed:	0

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

Enabling AWS Logs

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

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

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

To enable AWS logs in SonicOS:

1. Navigate to the **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 holds the logs sent to AWS CloudWatch Logs.
5. The logs are sent at the specified **Synchronization Interval**. Change the value of the interval (in seconds) to suit your needs.
6. Optionally, you can click **FORCE SYNC** to manually synchronize with your AWS Console settings.
7. Click **ACCEPT**.

10

Configuring Secondary Storage

Introduction

Specific models of SonicWall NS*a* firewalls include Built-In Storage Modules. Capacities range from 16GB to 256GB:

Product Model and Built-In Storage Module Capacity

NS*a* 2650	16GB
NS*a* 3650	32GB
NS*a* 4650	32GB
NS*a* 5650	64GB
NS*a* 6650	64GB
NS*a* 9250*	128GB
NS*a* 9450*	128GB
NS*a* 9650*	256GB

* Includes 1 TB Flexible Storage Module as standard configuration.

A 1TB Flexible Storage Module comes standard with the NS*a* 9250—9660 models. It can also be optionally acquired to support the NS*a* 2650—6650 models. Importantly, the Flexible Storage Module can be moved from one NS*a* firewall to another.

The NS*a* firewalls store syslog and trace log entries to these modules. By default, these logs are sent to the Built-In Storage Module. Administrators can configure the Flexible Storage Module as the primary target for log storage (see Configuring Storage Options on page 103).

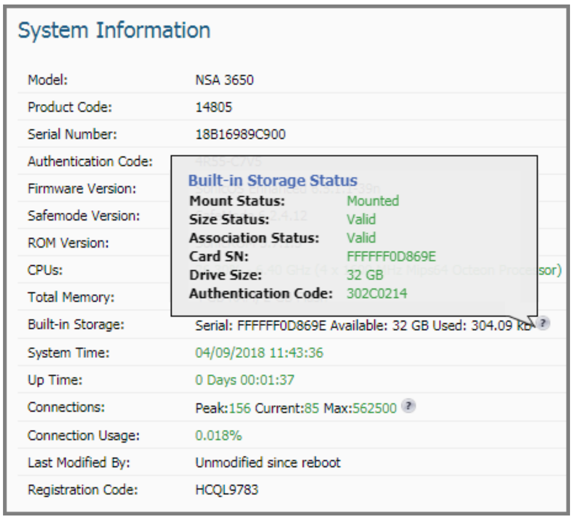
When the firewall is running, these logs are maintained in system memory. On a warm reset generated by software, the current database of up to 50,000 event log entires is written to a secondary storage module along with a set of trace message. Typically a trace log file is 1.28 MB times the number of CPUs in the firewall's processor core. In the event of a cold reset (pressing the front panel switch), logs currently in memory are lost. Depending on capacity, the storage modules accumulate multiple snapshots of the logs in system memory at the time of warm-resets.

Mounting the Storage Modules

△ **CAUTION: The Flexible Storage Module is NOT hot-swapable. Be sure to power down the firewall before removing or replacing this memory module.**

Built-In Modules

When the firewall boots, it checks its serial number and the serial number of the Built-In Module and works with the License Manager and MySonicWall to ensure they are properly associated. If so, the Module will appear in the **Monitor | Current Status > System Status** with **Association Status: Valid**. If there is a problem with association, or the storage module is under RMA an error message will appear in the System Information panel.



System Information

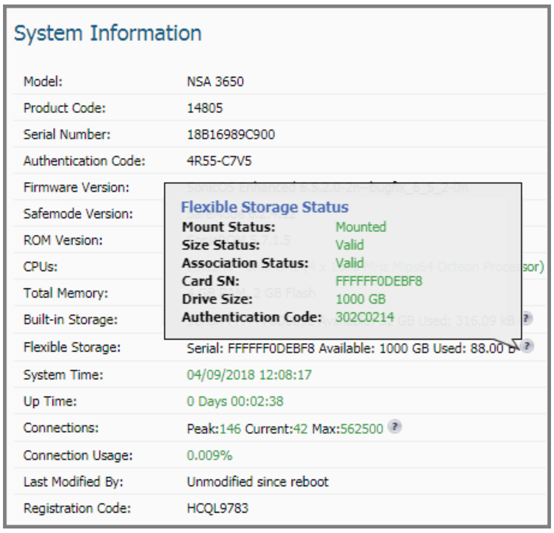
Model:	NSA 3650
Product Code:	14805
Serial Number:	18B16989C900
Authentication Code:	
Firmware Version:	
Safemode Version:	
ROM Version:	
CPUs:	sor)
Total Memory:	
Built-in Storage:	Serial: FFFFFF0D869E Available: 32 GB Used: 304.09 kB
System Time:	04/09/2018 11:43:36
Up Time:	0 Days 00:01:37
Connections:	Peak:156 Current:85 Max:562500
Connection Usage:	0.018%
Last Modified By:	Unmodified since reboot
Registration Code:	HCQL9783

Built-in Storage Status

Mount Status:	Mounted
Size Status:	Valid
Association Status:	Valid
Card SN:	FFFFFF0D869E
Drive Size:	32 GB
Authentication Code:	302C0214

Flexible Modules

When the firewall boots, it reports the serial number of the Flexible Storage Module to the License Manager and MySonicWall to ensure it has not been found defective and is therefore covered by a Return Materials Authorization (RMA). Normally the Flexible Storage Module is activated, and will appear in the **Monitor | Current Status > System Status** with **Association Status: Valid**.



System Information

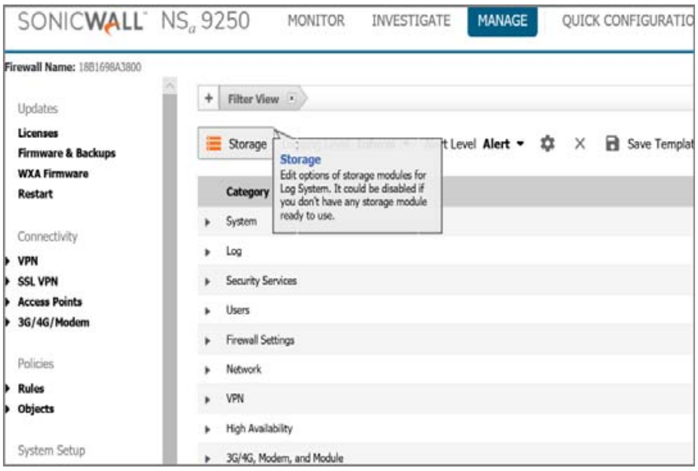
Model:	NSA 3650
Product Code:	14805
Serial Number:	18B16989C900
Authentication Code:	4R55-C7V5
Firmware Version:	
Safemode Version:	
ROM Version:	
CPUs:	sor)
Total Memory:	
Built-in Storage:	
Flexible Storage:	Serial: FFFFFF0DEBF8 Available: 1000 GB Used: 88.00 B
System Time:	04/09/2018 12:08:17
Up Time:	0 Days 00:02:38
Connections:	Peak:146 Current:42 Max:562500
Connection Usage:	0.009%
Last Modified By:	Unmodified since reboot
Registration Code:	HCQL9783

Flexible Storage Status

Mount Status:	Mounted
Size Status:	Valid
Association Status:	Valid
Card SN:	FFFFFF0DEBF8
Drive Size:	1000 GB
Authentication Code:	302C0214

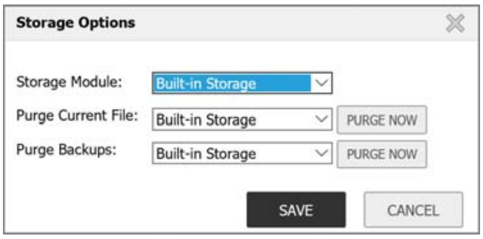
Configuring Storage Options

To define which storage module the logs go to, go to **MANAGE | Logs and Reporting > Log Settings > Base Setup**.



Storage
Edit options of storage modules for Log System. It could be disabled if you don't have any storage module ready to use.

In the dialog box that comes up, you can choose which secondary storage module to direct logs to and purge existing logs: either the current log presently in system memory, or the logs that are already in place on the storage module.



Storage Options

Storage Module: Built-in Storage

Purge Current File: Built-in Storage PURGE NOW

Purge Backups: Built-in Storage PURGE NOW

Viewing Event Logs

For details on filtering the event logs, refer to Filtering the Base Setup View on page 49.

Log Monitoring

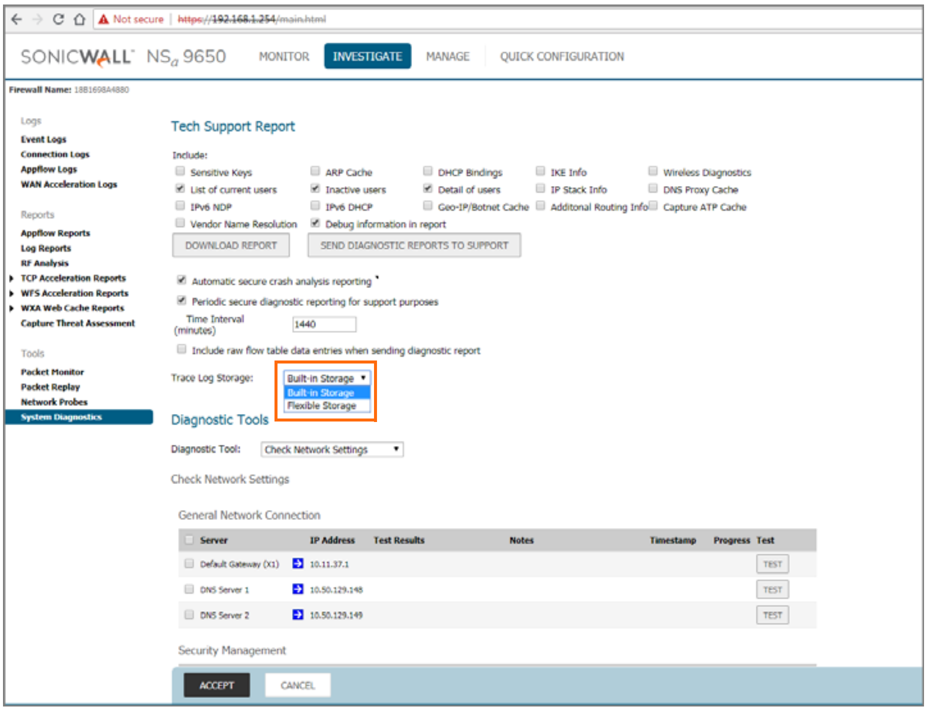
Log monitoring features described in the chapters listed below can be applied to logs in the secondary storage modules:

- Configuring Log Settings on page 48
- Configuring Syslog Settings on page 71
- Configuring Log Automation on page 81

Viewing Trace Logs

To View Trace Logs:

1 Go to **INVESTIGATE > System Diagnostics** page. In the Trace Log Storage drop-down list select desired module option.



Not secure | https://192.168.1.254/main.html

SONICWALL NS$_a$ 9650 MONITOR INVESTIGATE MANAGE QUICK CONFIGURATION

Firewall Name: 18B1698A4880

Logs
Event Logs
Connection Logs
Appflow Logs
WAN Acceleration Logs

Reports
Appflow Reports
Log Reports
RF Analysis
TCP Acceleration Reports
WFS Acceleration Reports
WXA Web Cache Reports
Capture Threat Assessment

Tools
Packet Monitor
Packet Replay
Network Probes
System Diagnostics

Tech Support Report

Include:

□ Sensitive Keys	□ ARP Cache	□ DHCP Bindings	□ IKE Info	□ Wireless Diagnostics
☑ List of current users	☑ Inactive users	☑ Detail of users	□ IP Stack Info	□ DNS Proxy Cache
□ IPv6 NDP	□ IPv6 DHCP	□ Geo-IP/Botnet Cache	□ Additonal Routing Info	□ Capture ATP Cache
□ Vendor Name Resolution	☑ Debug information in report			

DOWNLOAD REPORT | SEND DIAGNOSTIC REPORTS TO SUPPORT

☑ Automatic secure crash analysis reporting *

☑ Periodic secure diagnostic reporting for support purposes

Time Interval (minutes): 1440

□ Include raw flow table data entries when sending diagnostic report

Trace Log Storage: Built-in Storage
Built-in Storage
Flexible Storage

Diagnostic Tools

Diagnostic Tool: Check Network Settings

Check Network Settings

General Network Connection

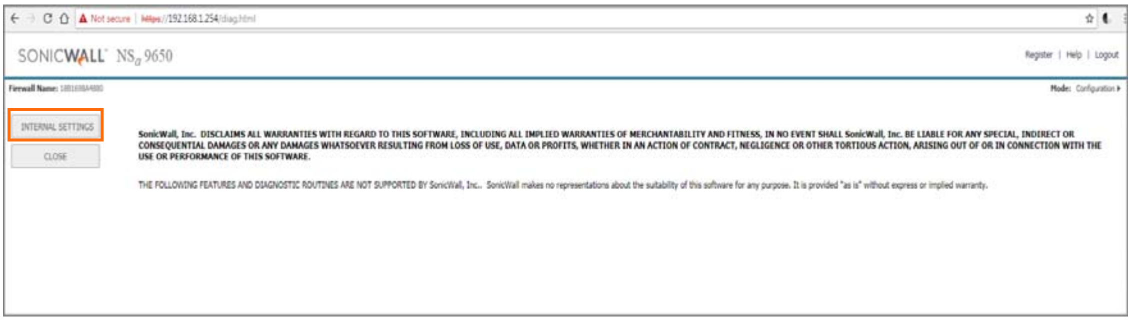
	Server	IP Address	Test Results	Notes	Timestamp	Progress	Test
□	Default Gateway (X1)	10.11.37.1					TEST
□	DNS Server 1	10.50.129.148					TEST
□	DNS Server 2	10.50.129.149					TEST

Security Management

ACCEPT | CANCEL

2 Click accept.

3 To download trace logs, go to *diag.html* page and then click on **Internal Settings** tab.



Not secure | https://192.168.1.254/diag.html

SONICWALL NS$_a$ 9650 Register | Help | Logout

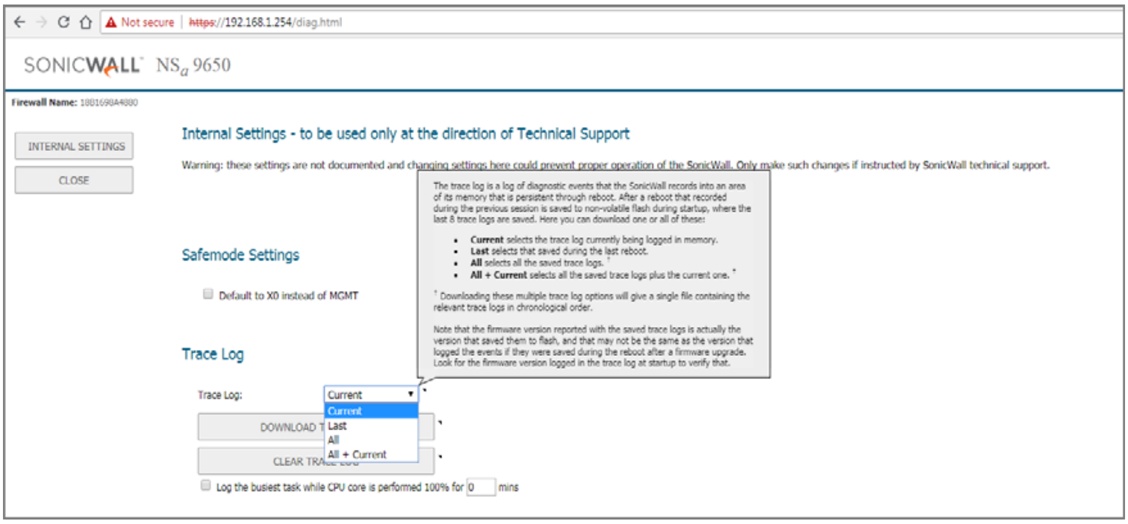
Firewall Name: 18B1698A4880 Mode: Configuration

INTERNAL SETTINGS
CLOSE

SonicWall, Inc. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SonicWall, Inc. BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

THE FOLLOWING FEATURES AND DIAGNOSTIC ROUTINES ARE NOT SUPPORTED BY SonicWall, Inc.. SonicWall makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

4 On Trace Log section select one of the options from the **Trace Log** field (**Last**/**All**/**All+Current**) and click on **DOWNLOAD TRACE LOG**.



Firewall Name: 18B1698A4880

Internal Settings - to be used only at the direction of Technical Support

Warning: these settings are not documented and changing settings here could prevent proper operation of the SonicWall. Only make such changes if instructed by SonicWall technical support.

The trace log is a log of diagnostic events that the SonicWall records into an area of its memory that is persistent through reboot. After a reboot that recorded during the previous session is saved to non-volatile flash during startup, where the last 8 trace logs are saved. Here you can download one or all of these:

- **Current** selects the trace log currently being logged in memory.
- **Last** selects that saved during the last reboot.
- **All** selects all the saved trace logs. †
- **All + Current** selects all the saved trace logs plus the current one. †

† Downloading these multiple trace log options will give a single file containing the relevant trace logs in chronological order.

Note that the firmware version reported with the saved trace logs is actually the version that saved them to flash, and that may not be the same as the version that logged the events if they were saved during the reboot after a firmware upgrade. Look for the firmware version logged in the trace log at startup to verify that.

Safemode Settings

□ Default to X0 instead of MGMT

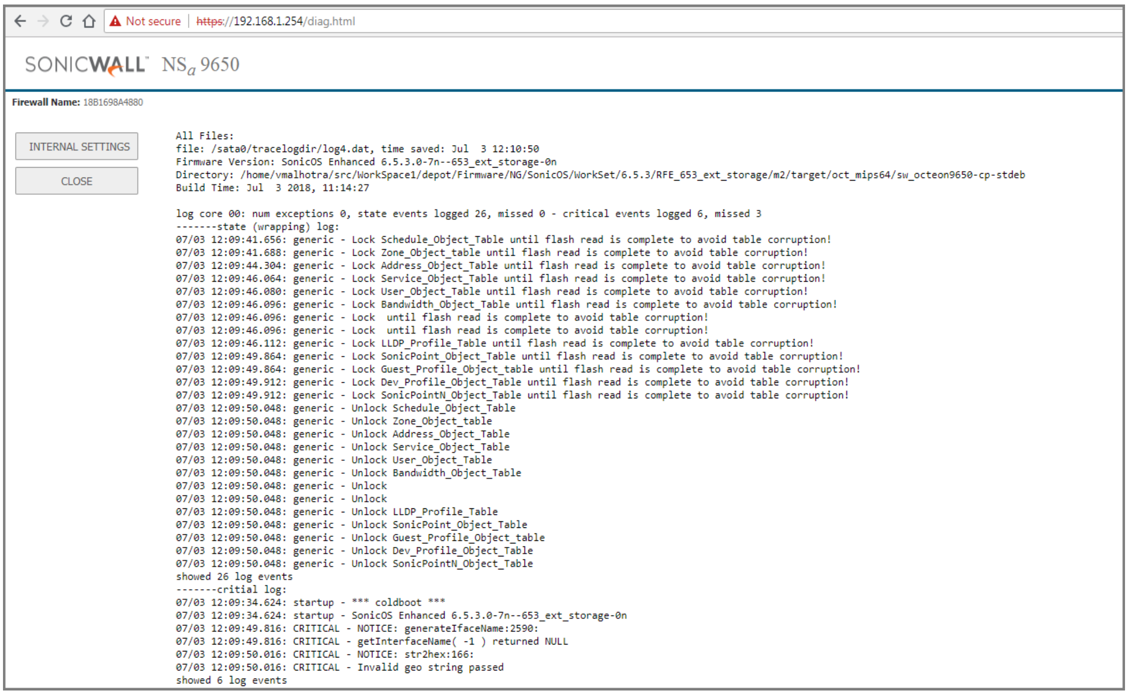
Trace Log

Trace Log: Current ▾
Current
Last
All
All + Current

□ Log the busiest task while CPU core is performed 100% for 0 mins

5 Click OK on the prompt: "**You are about to export trace log information in plaintext format. Continue?**"

The trace log information is then downloaded and shown in the diag.html page. If the external storage is functional and there has been a warm reboot, the page should show trace logs from the external storage device: the trace log file path should contain "/sata0" or "/sata1".



Firewall Name: 18B1698A4880

```
All Files:
file: /sata0/tracelogdir/log4.dat, time saved: Jul  3 12:10:50
Firmware Version: SonicOS Enhanced 6.5.3.0-7n--653_ext_storage-0n
Directory: /home/vmalhotra/src/WorkSpace1/depot/Firmware/NG/SonicOS/WorkSet/6.5.3/RFE_653_ext_storage/m2/target/oct_mips64/sw_octeon9650-cp-stdeb
Build Time: Jul  3 2018, 11:14:27

log core 00: num exceptions 0, state events logged 26, missed 0 - critical events logged 6, missed 3
-------state (wrapping) log:
07/03 12:09:41.656: generic - Lock Schedule_Object_Table until flash read is complete to avoid table corruption!
07/03 12:09:41.688: generic - Lock Zone_Object_table until flash read is complete to avoid table corruption!
07/03 12:09:44.304: generic - Lock Address_Object_Table until flash read is complete to avoid table corruption!
07/03 12:09:46.064: generic - Lock Service_Object_Table until flash read is complete to avoid table corruption!
07/03 12:09:46.080: generic - Lock User_Object_Table until flash read is complete to avoid table corruption!
07/03 12:09:46.096: generic - Lock Bandwidth_Object_Table until flash read is complete to avoid table corruption!
07/03 12:09:46.096: generic - Lock  until flash read is complete to avoid table corruption!
07/03 12:09:46.096: generic - Lock  until flash read is complete to avoid table corruption!
07/03 12:09:46.112: generic - Lock LLDP_Profile_Table until flash read is complete to avoid table corruption!
07/03 12:09:49.864: generic - Lock SonicPoint_Object_Table until flash read is complete to avoid table corruption!
07/03 12:09:49.864: generic - Lock Guest_Profile_Object_table until flash read is complete to avoid table corruption!
07/03 12:09:49.912: generic - Lock Dev_Profile_Object_Table until flash read is complete to avoid table corruption!
07/03 12:09:49.912: generic - Lock SonicPointN_Object_Table until flash read is complete to avoid table corruption!
07/03 12:09:50.048: generic - Unlock Schedule_Object_Table
07/03 12:09:50.048: generic - Unlock Zone_Object_table
07/03 12:09:50.048: generic - Unlock Address_Object_Table
07/03 12:09:50.048: generic - Unlock Service_Object_Table
07/03 12:09:50.048: generic - Unlock User_Object_Table
07/03 12:09:50.048: generic - Unlock Bandwidth_Object_Table
07/03 12:09:50.048: generic - Unlock
07/03 12:09:50.048: generic - Unlock
07/03 12:09:50.048: generic - Unlock LLDP_Profile_Table
07/03 12:09:50.048: generic - Unlock SonicPoint_Object_Table
07/03 12:09:50.048: generic - Unlock Guest_Profile_Object_table
07/03 12:09:50.048: generic - Unlock Dev_Profile_Object_Table
07/03 12:09:50.048: generic - Unlock SonicPointN_Object_Table
showed 26 log events
-------critial log:
07/03 12:09:34.624: startup - *** coldboot ***
07/03 12:09:34.624: startup - SonicOS Enhanced 6.5.3.0-7n--653_ext_storage-0n
07/03 12:09:49.816: CRITICAL - NOTICE: generateIfaceName:2590:
07/03 12:09:49.816: CRITICAL - getInterfaceName( -1 ) returned NULL
07/03 12:09:50.016: CRITICAL - NOTICE: str2hex:166:
07/03 12:09:50.016: CRITICAL - Invalid geo string passed
showed 6 log events
```

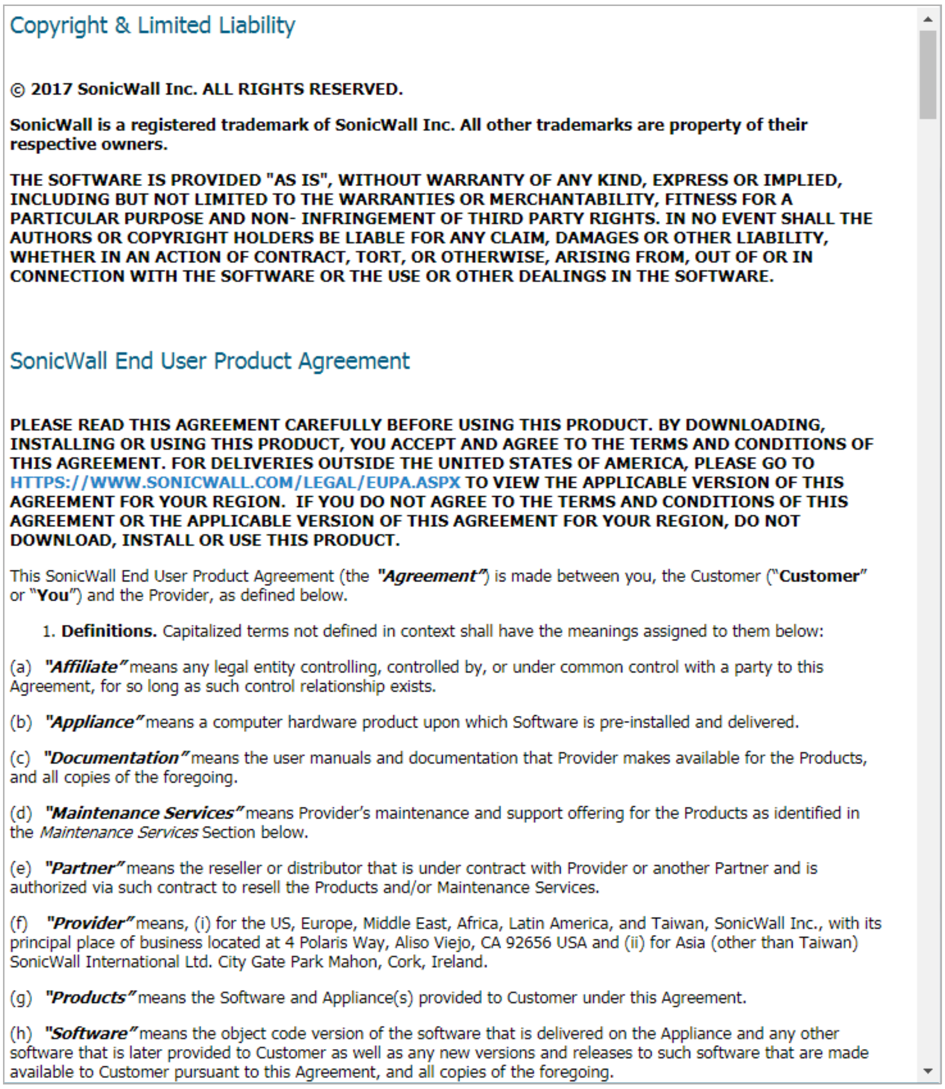
Part 3

Logs & Reporting | Legal and Support

11

Accessing Legal Information

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



Copyright & Limited Liability

© 2017 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a registered trademark of SonicWall Inc. All other trademarks are property of their respective owners.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON- INFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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.ASPX TO 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.

This 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.

12

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 Administration
Updated - November 2019
Software Version - 6.5.4
232-002065-04 Rev C

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

For more information, visit https://www.SonicWall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.SonicWall.com/en-us/legal/license-agreements.

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