SonicOS and SonicOSX 7

Device AppFlow

Administration Guide

SONICWALL®

Contents

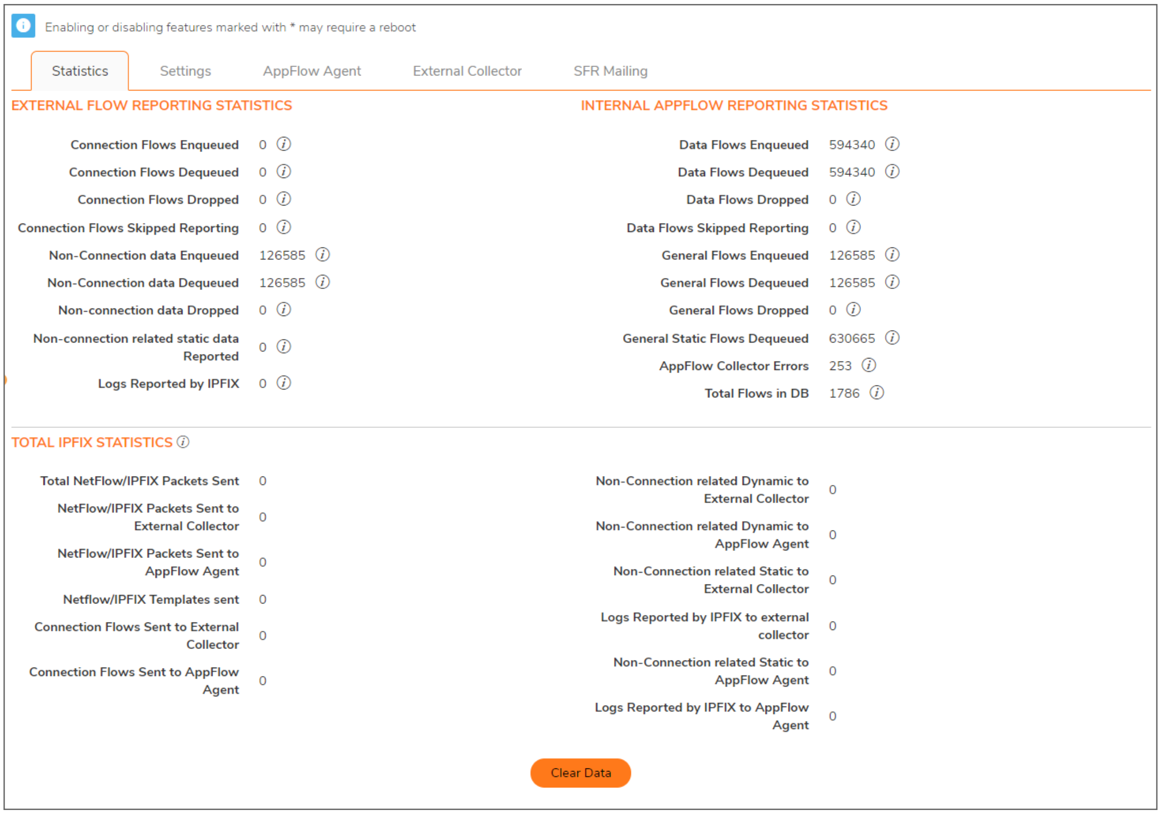
1

Flow Reporting

ⓘ | **NOTE:** References to SonicOS/X indicate that the functionality is available in both SonicOS and SonicOSX.

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 **DEVICE | AppFlow > 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 AppFlow Agents, External Collector reporting, and SonicFlow Report (SFR) Mailing settings.



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	126585
Non-Connection data Dequeued	126585
Non-connection data Dropped	0
Non-connection related static data Reported	0
Logs Reported by IPFIX	0

INTERNAL APPFLOW REPORTING STATISTICS

Data Flows Enqueued	594340
Data Flows Dequeued	594340
Data Flows Dropped	0
Data Flows Skipped Reporting	0
General Flows Enqueued	126585
General Flows Dequeued	126585
General Flows Dropped	0
General Static Flows Dequeued	630665
AppFlow Collector Errors	253
Total Flows in DB	1786

TOTAL IPFIX STATISTICS ⓘ

Total NetFlow/IPFIX Packets Sent	0
NetFlow/IPFIX Packets Sent to External Collector	0
NetFlow/IPFIX Packets Sent to AppFlow Agent	0
Netflow/IPFIX Templates sent	0
Connection Flows Sent to External Collector	0
Connection Flows Sent to AppFlow Agent	0
Non-Connection related Dynamic to External Collector	0
Non-Connection related Dynamic to AppFlow Agent	0
Non-Connection related Static to External Collector	0
Logs Reported by IPFIX to external collector	0
Non-Connection related Static to AppFlow Agent	0
Logs Reported by IPFIX to AppFlow Agent	0

You can access the AppFlow Reports page by enabling **Enable Aggregate AppFlow Report Data Collection** on the **DEVICE | AppFlow > Flow Reporting | Settings** page.

You can clear the AppFlow settings on each page back to their default values by clicking **Default Settings** at the bottom of each **DEVICE | AppFlow > Flow Reporting** tabs.

The **DEVICE | AppFlow > Flow Reporting** page has these tabs:

Statistics – Displays reporting statistics in four tables.

Settings – Allows the enabling of various real-time data collection and AppFlow report collection.

AppFlow Agent – Allows the configuring of AppFlow reporting to a AppFlow Agent.

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).

Topics:

- Statistics
- Settings
- AppFlow Agent
- External Collector
- SFR Mailing
- NetFlow Activation and Deployment Information
- User Configuration Tasks
- NetFlow Tables

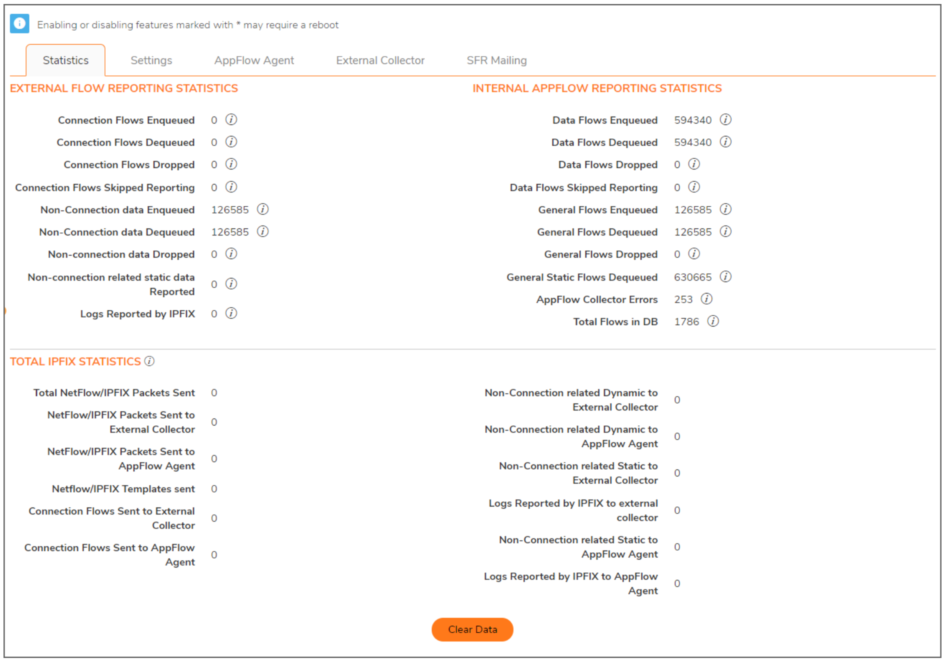
Statistics

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



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	126585
Non-Connection data Dequeued	126585
Non-connection data Dropped	0
Non-connection related static data Reported	0
Logs Reported by IPFIX	0

INTERNAL APPFLOW REPORTING STATISTICS

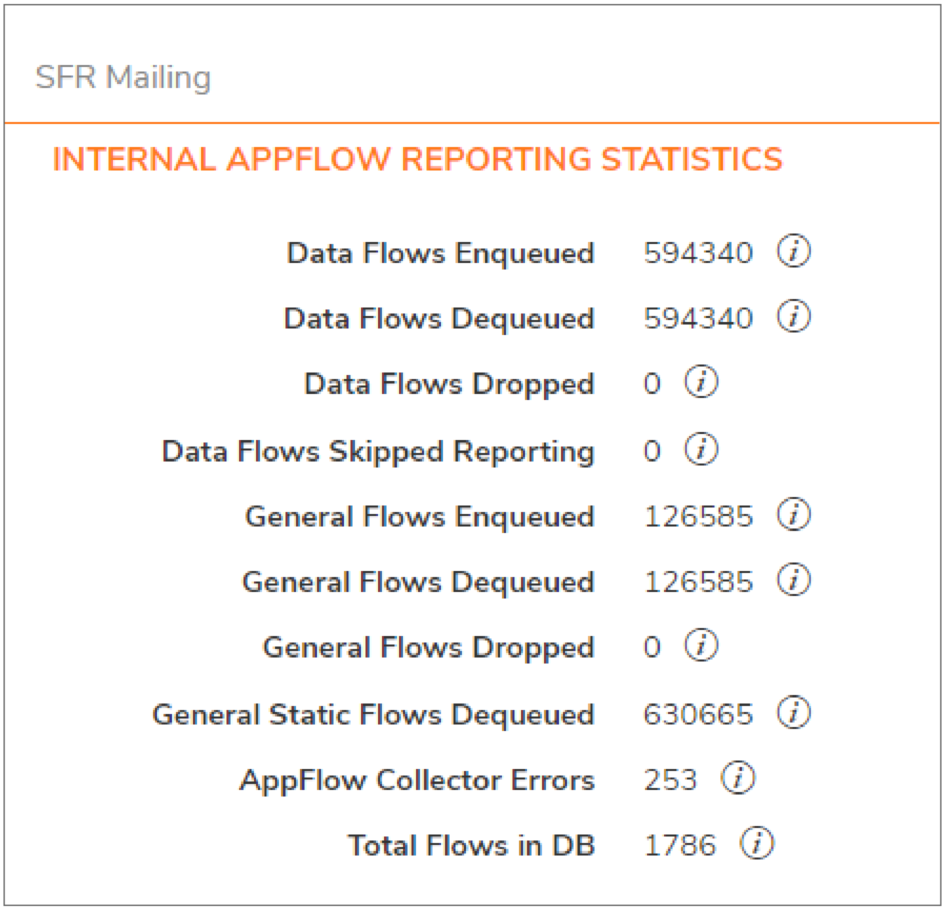
Data Flows Enqueued	594340
Data Flows Dequeued	594340
Data Flows Dropped	0
Data Flows Skipped Reporting	0
General Flows Enqueued	126585
General Flows Dequeued	126585
General Flows Dropped	0
General Static Flows Dequeued	630665
AppFlow Collector Errors	253
Total Flows in DB	1786

TOTAL IPFIX STATISTICS

Total NetFlow/IPFIX Packets Sent	0	Non-Connection related Dynamic to External Collector	0
NetFlow/IPFIX Packets Sent to External Collector	0	Non-Connection related Dynamic to AppFlow Agent	0
NetFlow/IPFIX Packets Sent to AppFlow Agent	0	Non-Connection related Static to External Collector	0
Netflow/IPFIX Templates sent	0	Logs Reported by IPFIX to external collector	0
Connection Flows Sent to External Collector	0	Non-Connection related Static to AppFlow Agent	0
Connection Flows Sent to AppFlow Agent	0	Logs Reported by IPFIX to AppFlow Agent	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



SFR Mailing

INTERNAL APPFLOW REPORTING STATISTICS

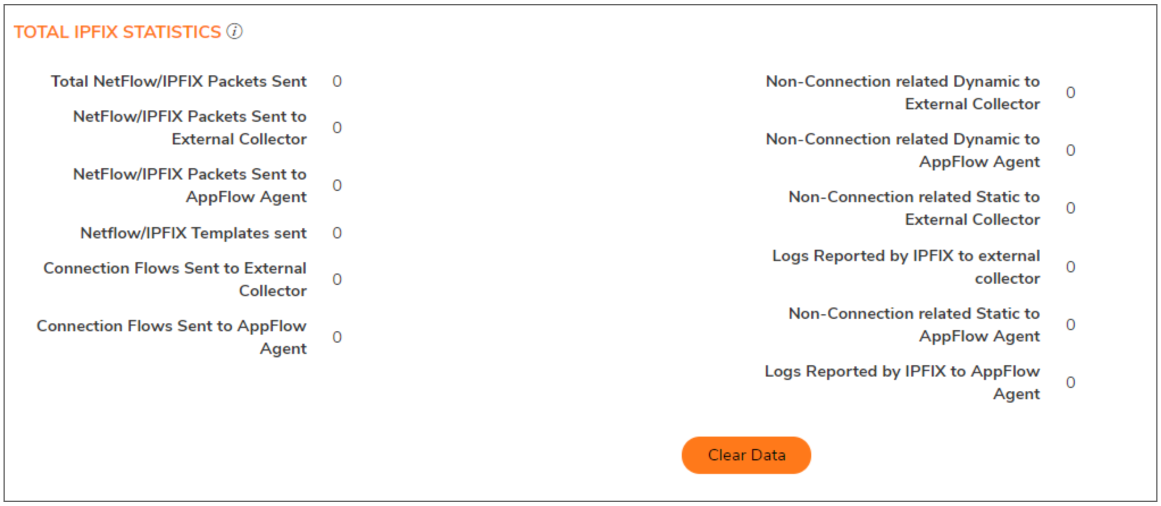
Data Flows Enqueued	594340 ⓘ
Data Flows Dequeued	594340 ⓘ
Data Flows Dropped	0 ⓘ
Data Flows Skipped Reporting	0 ⓘ
General Flows Enqueued	126585 ⓘ
General Flows Dequeued	126585 ⓘ
General Flows Dropped	0 ⓘ
General Static Flows Dequeued	630665 ⓘ
AppFlow Collector Errors	253 ⓘ
Total Flows in DB	1786 ⓘ

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 AppFlow Agent 0

Netflow/IPFIX Templates sent 0

Connection Flows Sent to External Collector 0

Connection Flows Sent to AppFlow Agent 0

Non-Connection related Dynamic to External Collector 0

Non-Connection related Dynamic to AppFlow Agent 0

Non-Connection related Static to External Collector 0

Logs Reported by IPFIX to external collector 0

Non-Connection related Static to AppFlow Agent 0

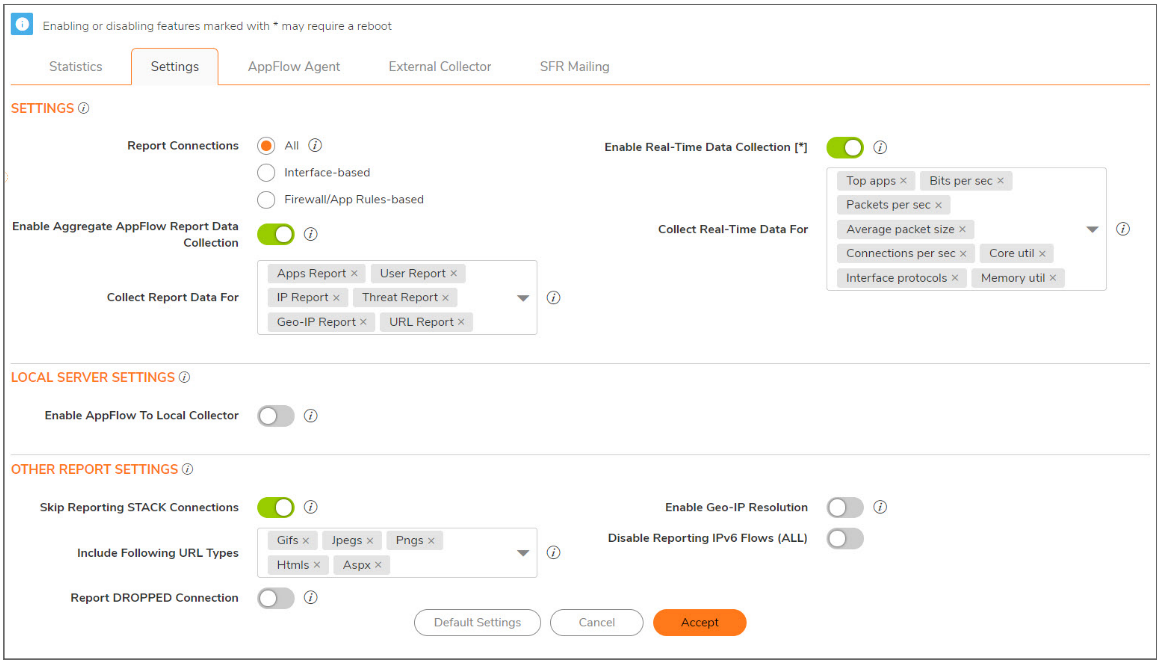
Logs Reported by IPFIX to AppFlow Agent 0

This statistic	Displays the total number of
Total NetFlow/IPFIX Packets Sent:	IPFIX/NetFlow packets sent to the all/external collector/AppFlow server/AppFlow Agent 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 AppFlow Agent	IPFIX/NetFlow packets sent to the AppFlow Agent so far.
NetFlow/IPFIX Templates Sent	IPFIX/NetFlow templates sent to the all/external collector/AppFlow server/AppFlow Agent.
Connection Flows Sent to External Collector	Connection/static/general flows that have been reported to the, external collector.
Connection Flows Sent to AppFlow Agent	Connection/static/general flows that have been reported to the AppFlow Agent.
Non-Connection related Dynamic Flows Sent to External Collector:	IPFIX/NetFlow packets sent to the external collector so far.

This statistic	Displays the total number of
Non-Connection related Dynamic Flows Sent to AppFlow Agent:	IPFIX/NetFlow packets sent to the AppFlow Agent 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 AppFlow Agent:	Connection/static/general flows that have been reported to the AppFlow Agent.
Logs Reported by IPFIX to AppFlow Agent	Logs reported to the AppFlow Agent by IPFIX so far.

Settings

The **Settings** tab 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 Aggregate AppFlow Report Data Collection: On

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

Enable Real-Time Data Collection [*]: On

Collect Real-Time Data For: Top apps × Bits per sec × Packets per sec × Average packet size × Connections per sec × Core util × Interface protocols × Memory util ×

LOCAL SERVER SETTINGS

Enable AppFlow To Local Collector: Off

OTHER REPORT SETTINGS

Skip Reporting STACK Connections: On

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

Report DROPPED Connection: Off

Enable Geo-IP Resolution: Off

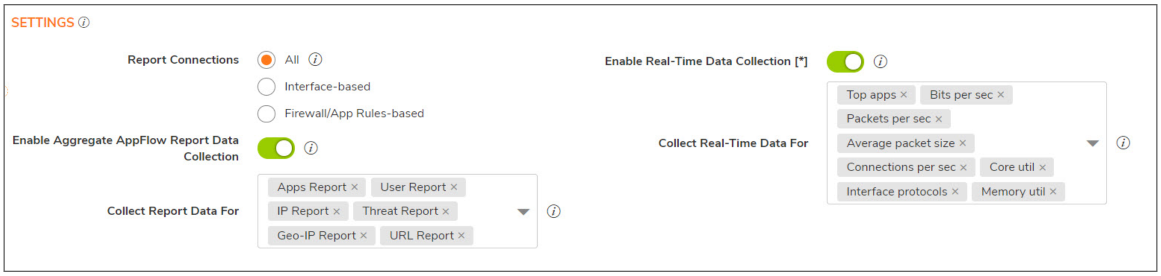
Disable Reporting IPv6 Flows (ALL): Off

Topics:

- Settings Configuration
- Local Server Settings
- Other Report Settings

Settings Configuration

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 Aggregate AppFlow Report Data Collection: ● On

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

Enable Real-Time Data Collection [*]: ● On

Collect Real-Time Data For: Top apps × Bits per sec × Packets per sec × Average packet size × Connections per sec × Core util × Interface protocols × Memory util ×

- **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 **POLICY | Rules and Policies > Access Rules** page and the **POLICY | Rules and Policies > 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 System Monitor does not collect or display streaming data as the real-time graphs displayed in the **MONITOR | Real-Time Charts > System Monitor** page is disabled.

- **Collect Real-Time Data For** — Select the streaming graphs to display on the **System 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** — If enabled, the firewall starts collecting data for aggregate reports. Individual items can be enabled/disabled in the next section. If disabled, AppFlow reports under the Dashboard are disabled.

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

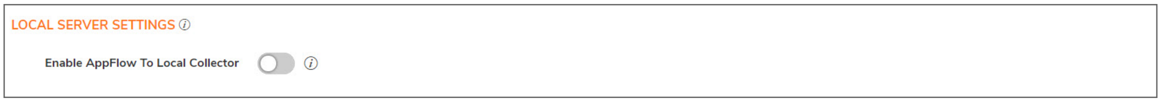
  ⓘ **TIP:** You can quickly display the **INVESTIGATE | Reports | AppFlow Reports** page by clicking the **Display** icon by **Enable Aggregate AppFlow Report Data Collection**.

  - **Collect Report Data For** — Enables/disables individual **Report Data Collection**. Select from this drop-down menu the data to display. 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 ⓘ

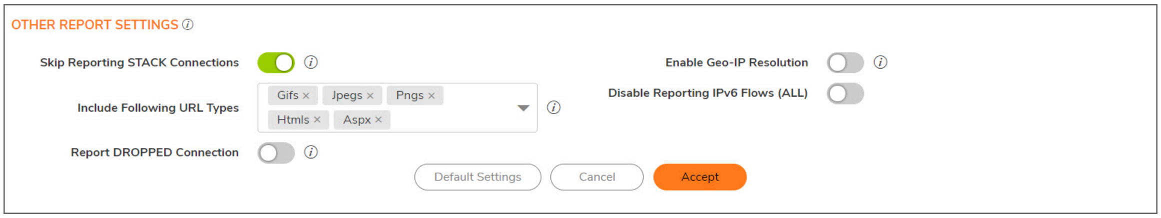
Enable AppFlow To Local Collector ○ ⓘ

Enable AppFlow To Local Collector Enables AppFlow reporting to internal collector. If disabled, the AppFlow Monitor under Dashboard 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

Skip Reporting STACK Connections ●

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

Report DROPPED Connection ○

Enable Geo-IP Resolution ○

Disable Reporting IPv6 Flows (ALL) ○

- **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.

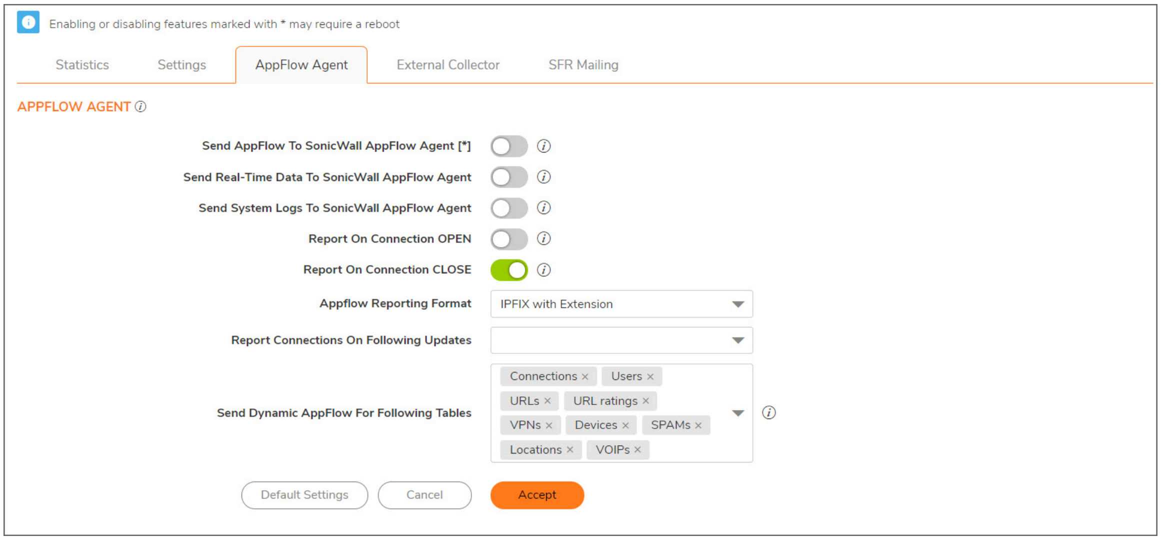
Gifs (selected by default)	**Jsons**
Jpegs (selected by default)	**Css**
Pngs (selected by default)	**Htmls** (selected by default)
Js	**Aspx** (selected by default)
Xmls	**Cms**

- **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.

  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 Agent

This screen allows you to send AppFlow and Real-time data to an AppFlow Agent. AppFlow Agents are SonicWall Flow Analytics, GMS, or NSM.



Enabling or disabling features marked with * may require a reboot

APPFLOW AGENT

Send AppFlow To SonicWall AppFlow Agent [*] ○
Send Real-Time Data To SonicWall AppFlow Agent ○
Send System Logs To SonicWall AppFlow Agent ○
Report On Connection OPEN ○
Report On Connection CLOSE ●
Appflow Reporting Format: IPFIX with Extension
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 AppFlow Agent** – The SonicWall appliance sends AppFlow data through IPFIX to a SonicWall AppFlow Agent. This option is not enabled by default.

  If this option is disabled, the SonicWall AppFlow Agent does not show AppFlow Monitor, AppFlow Report, and AppFlow Dashboard charts on the AppFlow Agent 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 AppFlow Agent** – The SonicWall appliance sends real-time data through IPFIX to the SonicWall AppFlow Agent. This option is disabled by default.

  If this option is disabled, the SonicWall AppFlow Agent does not display real-time charts on the AppFlow Agent or through redirection on a SonicWall appliance.

- **Send System Logs to SonicWall AppFlow Agent** – The SonicWall firewall sends system logs through IPFIX to the SonicWall AppFlow Agent. 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 AppFlow Agent 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 AppFlow Agent. All associated data related to that connection are available and reported. This option is enabled by default.
- **AppFlow Reporting Format** – Select either **IPFIX with Extension** or **IPFIX with Extension v2**.
- **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	**VPN tunnel detection**
application detection	**URL detection**

user detection

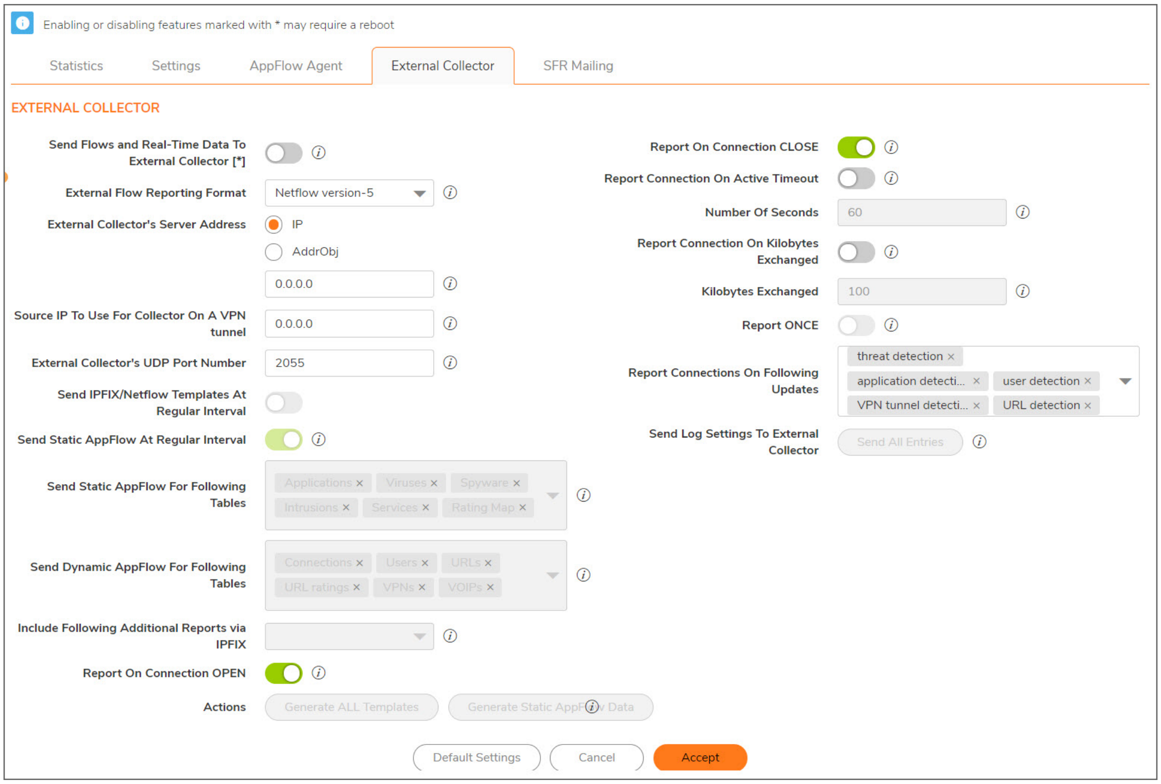
- **Send Dynamic AppFlow For Following Tables** – The firewall sends data for the selected tables. By default, all the tables are selected.

Connections	**Devices**
Users	**SPAMs**
URLs	**Locations**
URL ratings	**VOIPs**
VPNs	

> ⓘ **NOTE:** 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

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



Enabling or disabling features marked with * may require a reboot

EXTERNAL COLLECTOR

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

External Flow Reporting Format: Netflow version-5

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: off

Send Static AppFlow At Regular Interval: on

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: on

Actions: Generate ALL Templates | Generate Static AppFlow Data

Report On Connection CLOSE: on

Report Connection On Active Timeout: off

Number Of Seconds: 60

Report Connection On Kilobytes Exchanged: off

Kilobytes Exchanged: 100

Report ONCE: off

Report Connections On Following Updates: threat detection × application detecti... × user detection × VPN tunnel detecti... × URL detection ×

Send Log Settings To External Collector: Send All Entries

- **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**

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

  > **NOTE:** IPFIX with extensions v2 is still supported by enabling an internal setting. For instructions on how to enable this option, contact SonicWall Support. Currently, AppFlow Agent does not support this IPFIX version.

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

    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)	**Services** (selected by default)
Viruses (selected by default)	**Rating Map** (selected by default)
Spyware (selected by default)	**Table Map**
Intrusions (selected by default)	**Column Map**
Location Map	

When running in **IPFIX with extensions** mode, the firewall reports multiple types of data to an external device to correlate User, VPN, Application, Virus, and Spyware information. Data is both static and dynamic. Static tables are needed only once as they rarely change. Depending on the capability of the external collector, not all static tables are needed.

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

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

  NOTE: This option is available with **IPFIX with extensions** only. The firewall generates reports for the selected tables. As the firewall 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)	**Devices**
Users (selected by default)	**SPAMs**
URLs (selected by default)	**Locations**
URL ratings (selected by default)	**VoIPs** (selected by default)
VPNs (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**:

    - **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**:

    - **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.

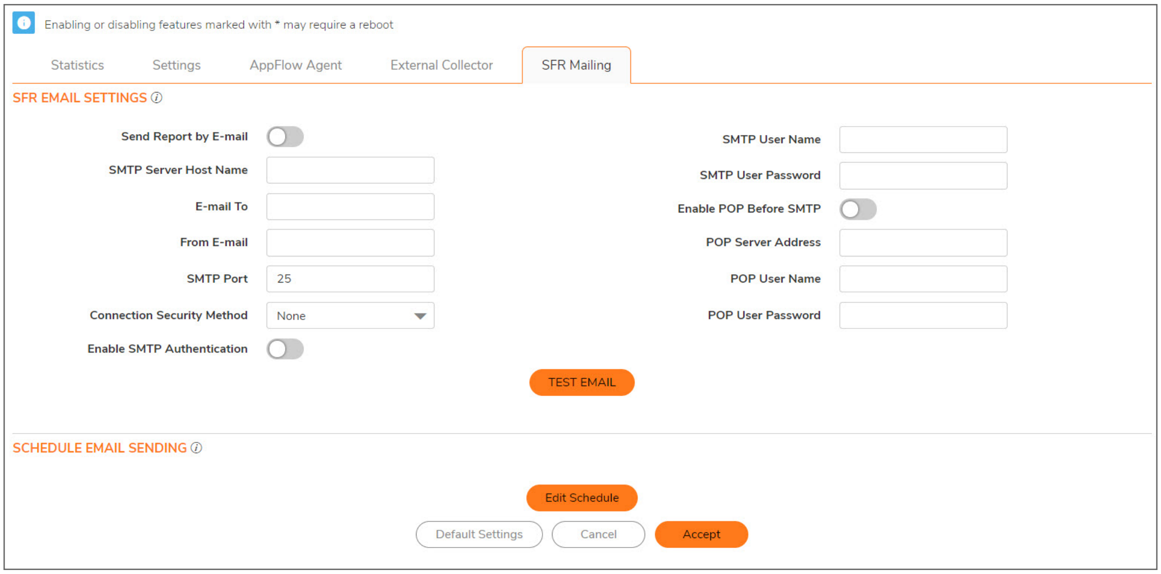
    ⓘ **NOTE:** This option is available with **IPFIX with extensions** only.
- **Log Settings To External Collector** — Sends the necessary fields of log settings to the external collector when you click **Send All Entries**.

  ⓘ **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**.
  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

Use the **SFR Mailing** tab 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 User Name	
SMTP Server Host Name		SMTP User Password	
E-mail To		Enable POP Before SMTP	○
From E-mail		POP Server Address	
SMTP Port	25	POP User Name	
Connection Security Method	None	POP User Password	
Enable SMTP Authentication	○		

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 **DEVICE | Appflow > 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:
   You need to verify the Email settings and try again.

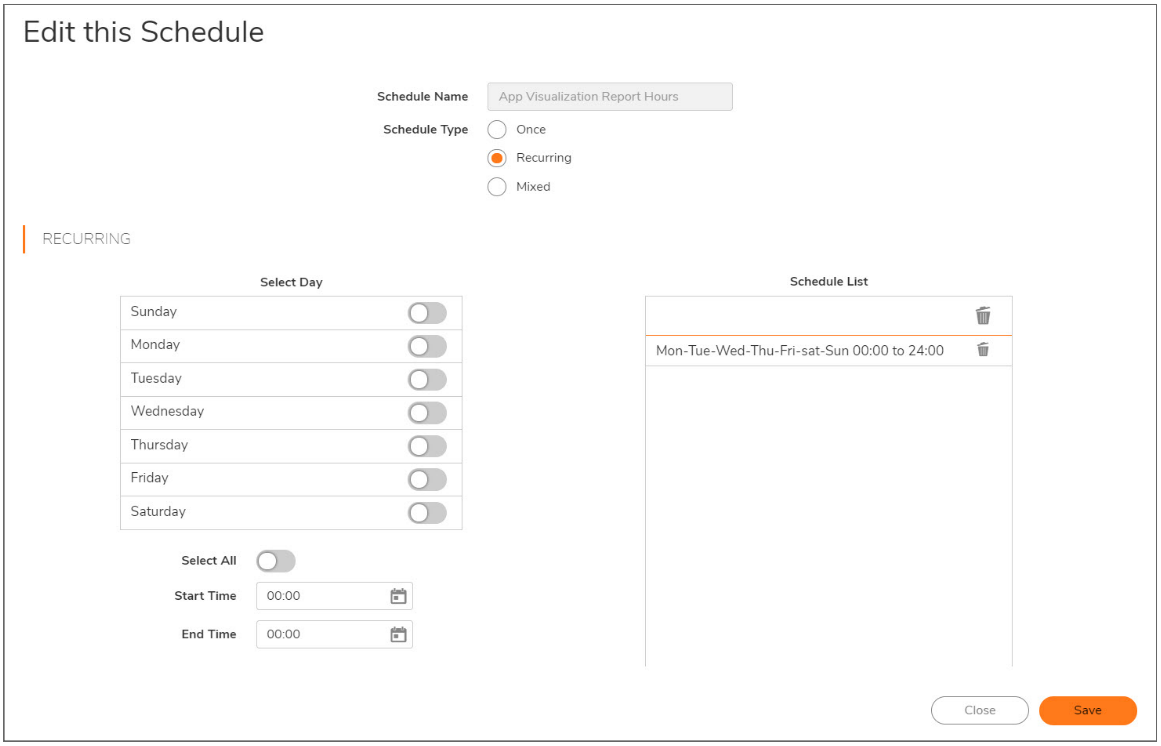
Scheduling SFR Reports by Email

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 **DEVICE | Appflow > 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**. The **Edit this Schedule** page displays.



Edit this Schedule

Schedule Name: App Visualization Report Hours

Schedule Type: ○ Once ● Recurring ○ Mixed

RECURRING

Start Time: 00:00

End Time: 00:00

Schedule List

Mon-Tue-Wed-Thu-Fri-sat-Sun 00:00 to 24:00

5. In the **Schedule Name** field, enter a name for your report.

6. 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.

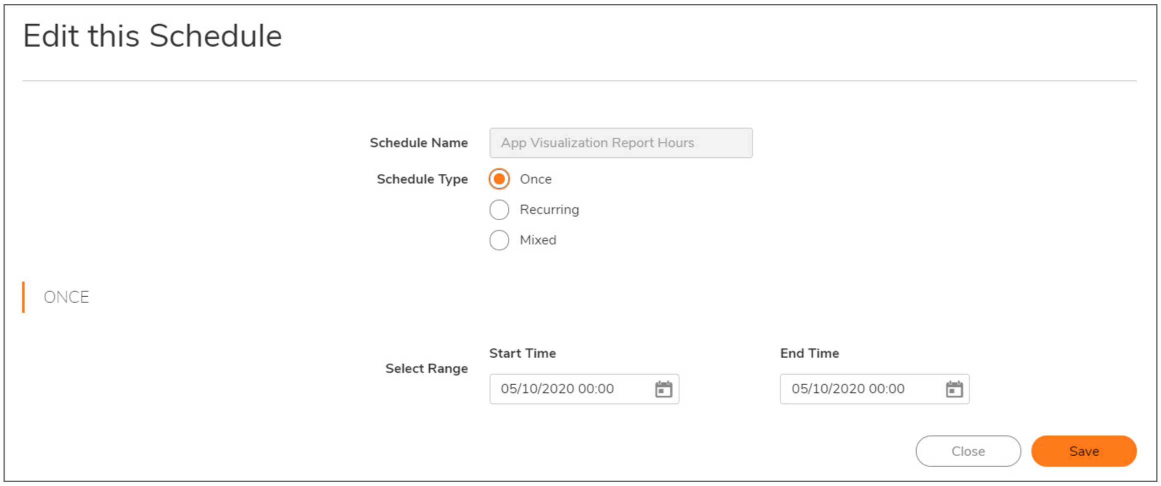
Topics:

- Scheduling One-Time Delivery of the SFR
- Scheduling Recurring Delivery of the SFR
- Deleting Scheduled Reports

Scheduling One-Time Delivery of the SFR

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

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



Edit this Schedule

Schedule Name: App Visualization Report Hours

Schedule Type: ● Once ○ Recurring ○ Mixed

ONCE

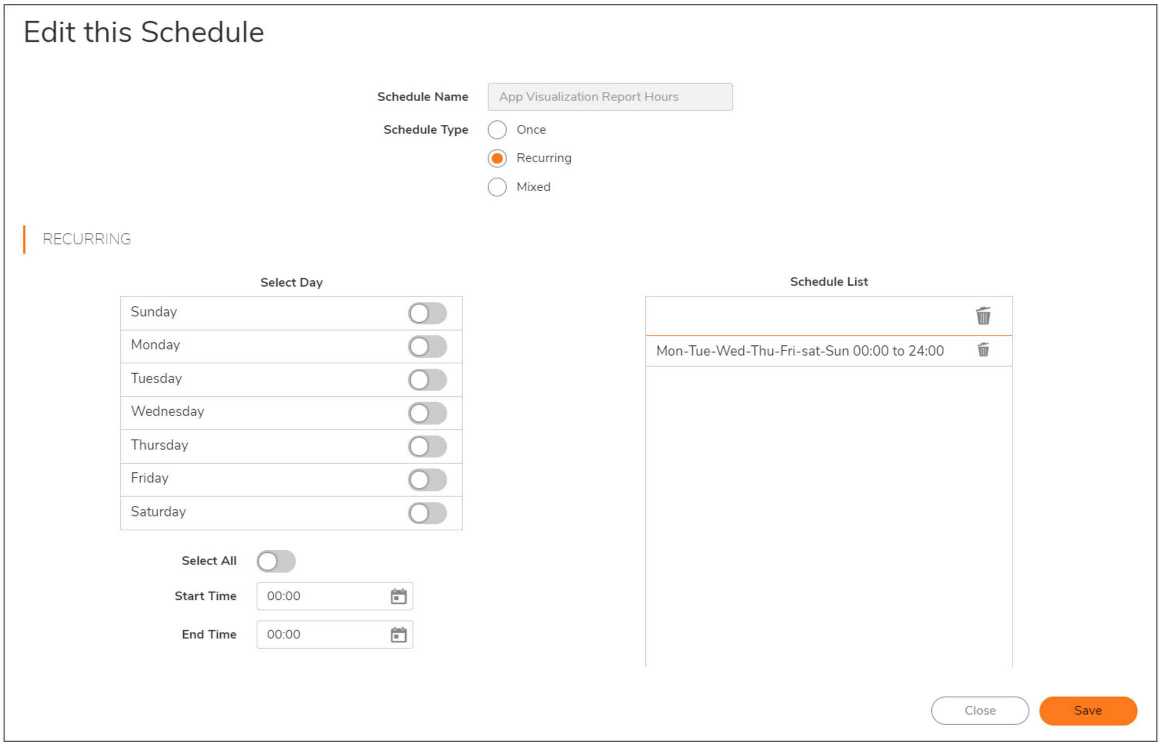
Select Range: Start Time 05/10/2020 00:00 End Time 05/10/2020 00:00

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 **Save.**

Scheduling Recurring Delivery of the SFR

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

1. For the **Schedule type**, select **Recurring**.
2. In the **Recurring** section:



Edit this Schedule

Schedule Name App Visualization Report Hours

Schedule Type ○ Once ● Recurring ○ Mixed

RECURRING

Select Day	
Sunday	○
Monday	○
Tuesday	○
Wednesday	○
Thursday	○
Friday	○
Saturday	○

Select All ○

Start Time 00:00

End Time 00:00

Schedule List
Mon-Tue-Wed-Thu-Fri-sat-Sun 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.

To delete selected scheduled reports:

1. Select the reports to be deleted in the **Schedule List**.
2. Click **Delete this Schedule** (small garbage can). The reports you selected are deleted from the list.

To delete all scheduled reports:

1. Click **Delete All** (Top Garbage can). All of the reports are deleted from the list.

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/X 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 AppFlow Agent 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**.
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** tab.
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**.

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

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

3. Click **External Collector**.
4. Select **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.
10. After the templates have been generated, click **Accept**.

Configuring IPFIX (NetFlow Version 10)

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

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

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

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

Configuring IPFIX with Extensions

To configure IPFIX with extensions flow reporting:

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

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

3. Click **External Collector**.
4. Select **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**.

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

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

    ⓘ **NOTE:** SonicOS/X 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 AppFlow Agent to Include Logs Through IPFIX

To configure AppFlow Agent to include logs through IPFIX:

1. Navigate to **DEVICE | AppFlow > Flow Reporting**.
2. Click **AppFlow Agent**.
3. Select **Send System Logs to SonicWall AppFlow Agent**. This option is not selected by default.
4. Click **Accept**.
5. Navigate to **DEVICE | AppFlow > AppFlow Agent**.
6. To send log messages to the AppFlow Agent, click **Synchronize Log Settings**.

ⓘ **IMPORTANT:** Ensure the connection between SonicOS/X on the firewall and the AppFlow Agent 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/X is upgraded, for example, with new log events.
- The connection between SonicOS/X (firewall) and the external server has been down for some time and log settings might have been edited during that time.

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

7. Click **Accept**.

Configuring Netflow with Extensions with SonicWall Scrutinizer

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

To verify your Netflow with Extensions reporting configurations:

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

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

    ⓘ **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 **NETWORK | System > Interfaces**.

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

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

16. Click **OK**.

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

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

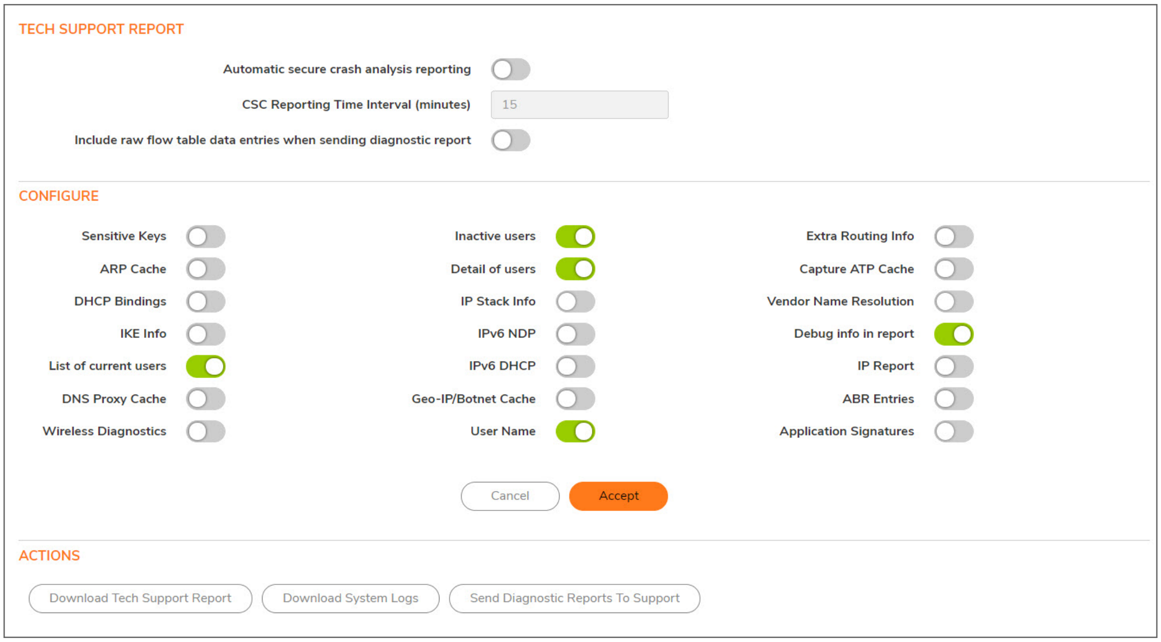
Unlike Static tables, the data of Dynamic tables change over time and are sent repeatedly, based on the activity of the firewall. The columns of these tables grow over time, with the exception of a few tables containing statistics or utilization reports. Exportable Dynamic IPFIX Tables lists the Dynamic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

This 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 **DEVICE | Diagnostics > Tech Support Report**, and clicking **Download Tech Support Report** in the **Actions** section.



TECH SUPPORT REPORT

Automatic secure crash analysis reporting ○

CSC Reporting Time Interval (minutes) 15

Include raw flow table data entries when sending diagnostic report ○

CONFIGURE

Sensitive Keys	○	Inactive users	●	Extra Routing Info	○
ARP Cache	○	Detail of users	●	Capture ATP Cache	○
DHCP Bindings	○	IP Stack Info	○	Vendor Name Resolution	○
IKE Info	○	IPv6 NDP	○	Debug info in report	●
List of current users	●	IPv6 DHCP	○	IP Report	○
DNS Proxy Cache	○	Geo-IP/Botnet Cache	○	ABR Entries	○
Wireless Diagnostics	○	User Name	●	Application Signatures	○

ACTIONS

Cancel
Accept
Download Tech Support Report
Download System Logs
Send Diagnostic Reports To Support

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 Header Format .

NETFLOW VERSION 5 HEADER FORMAT

Bytes	Content	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

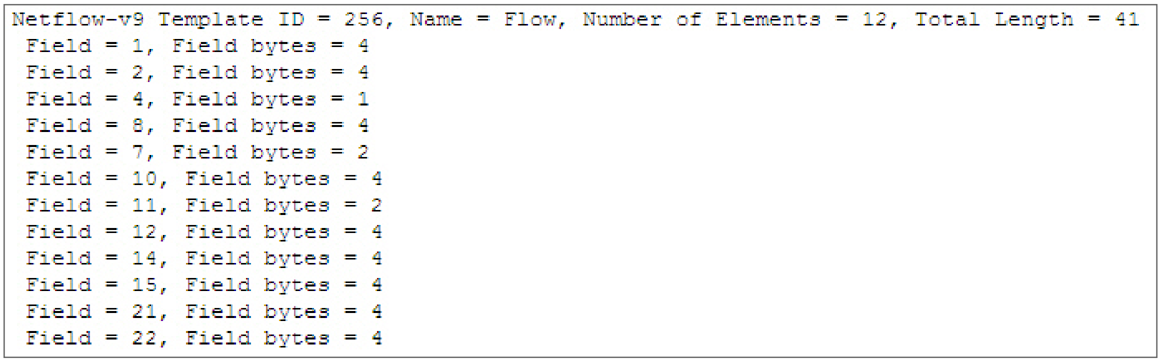
Bytes	Content	Description
20	engine_type	Type of flow-switching engine
20	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

NETFLOW VERSION 5 RECORD FORMAT

Bytes	Content	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
```

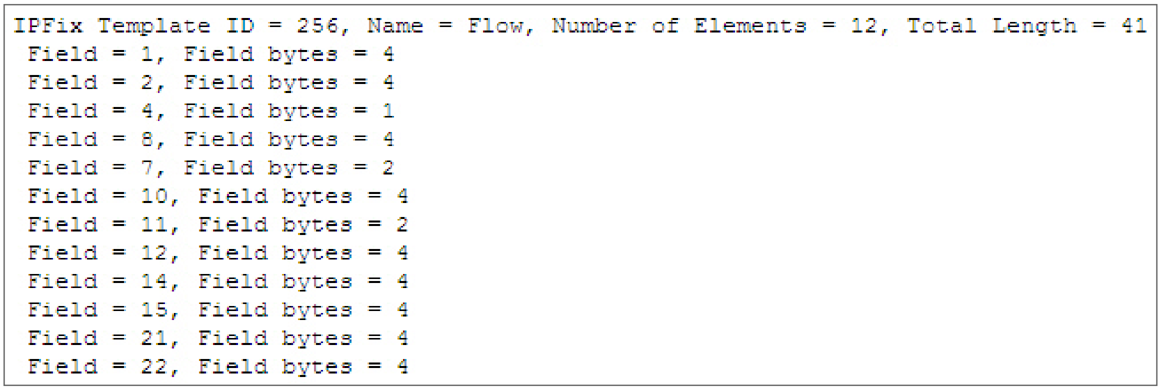
Netflow Version 9 Template FlowSet Fields details the NetFlow version 9 Template FlowSet field descriptions.

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.
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.

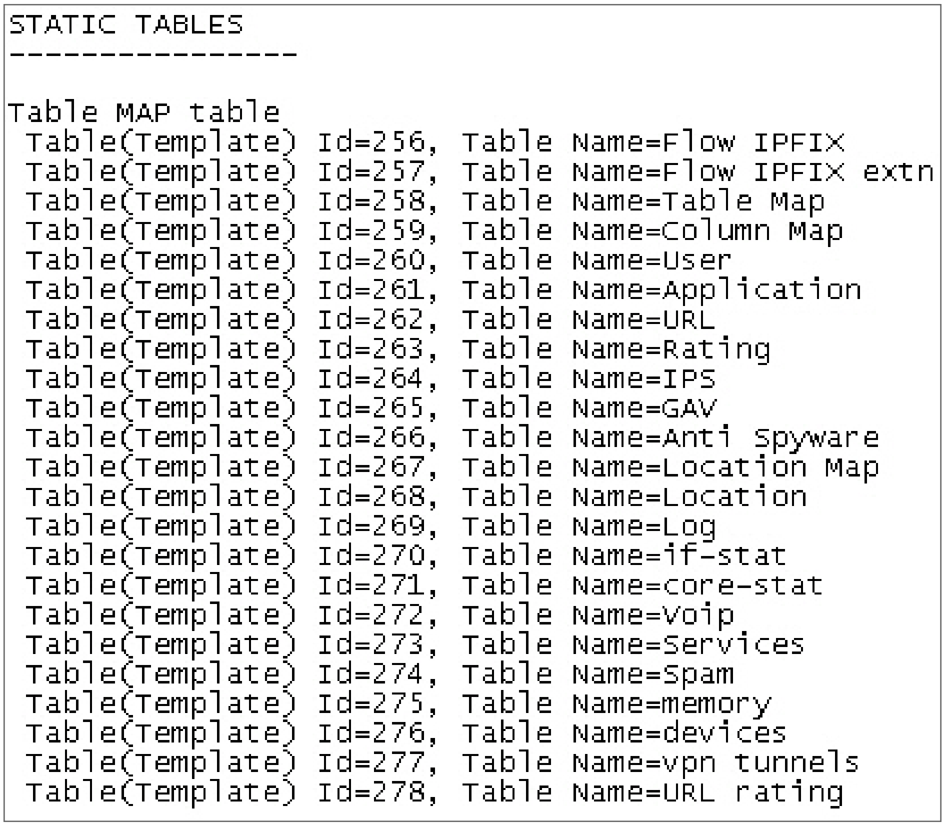
IPFIX with Extensions

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.

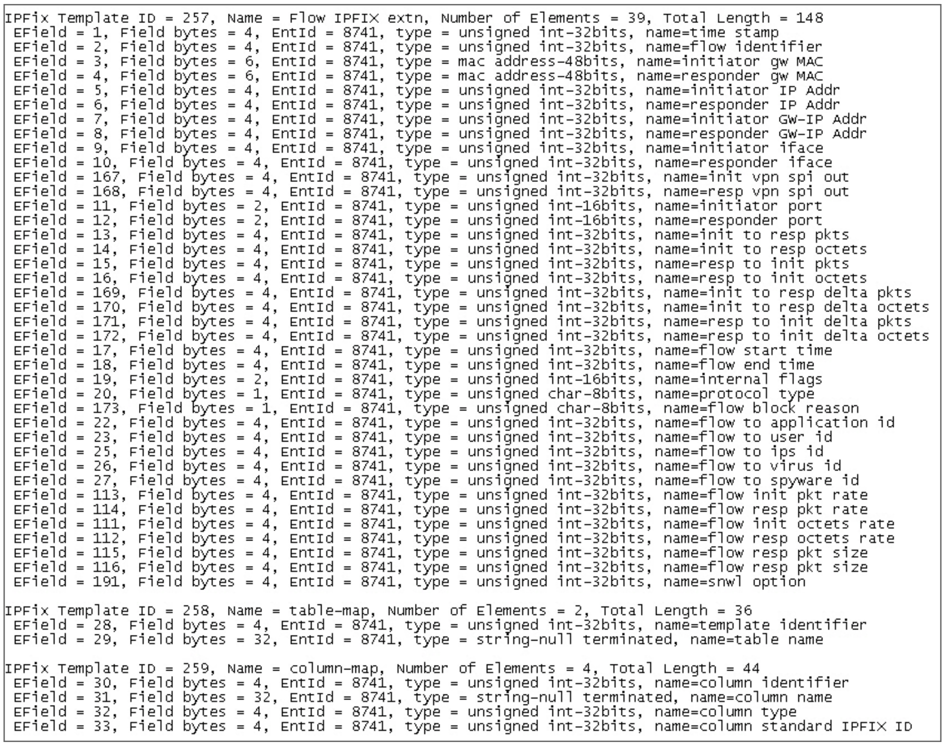
IPFIX WITH EXTENSIONS NAME TEMPLATE EXAMPLE



```
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
```

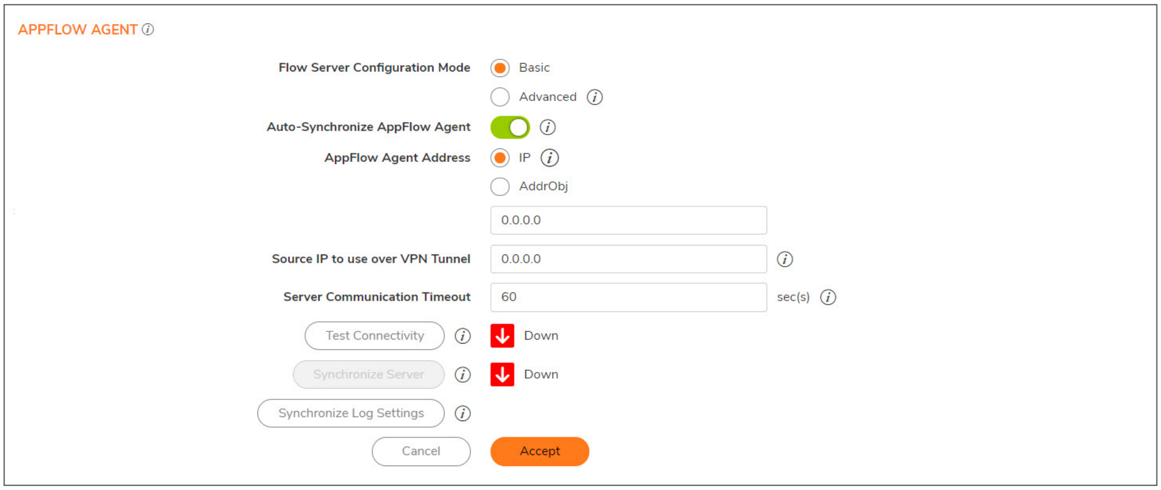
2

AppFlow Agent

This enables sending AppFlow and Real-Time data to the AppFlow Agent. An AppFlow Agent can either be a SonicWall Flow Analytics, GMS or NSM.

To send AppFlow and Real-Time data to your AppFlow Agent:

1. Navigate to **DEVICE | AppFlow > AppFlow Agent**.



APPFLOW AGENT

Flow Server Configuration Mode: ● Basic ○ Advanced

Auto-Synchronize AppFlow Agent: On

AppFlow Agent Address: ● IP ○ AddrObj

0.0.0.0

Source IP to use over VPN Tunnel: 0.0.0.0

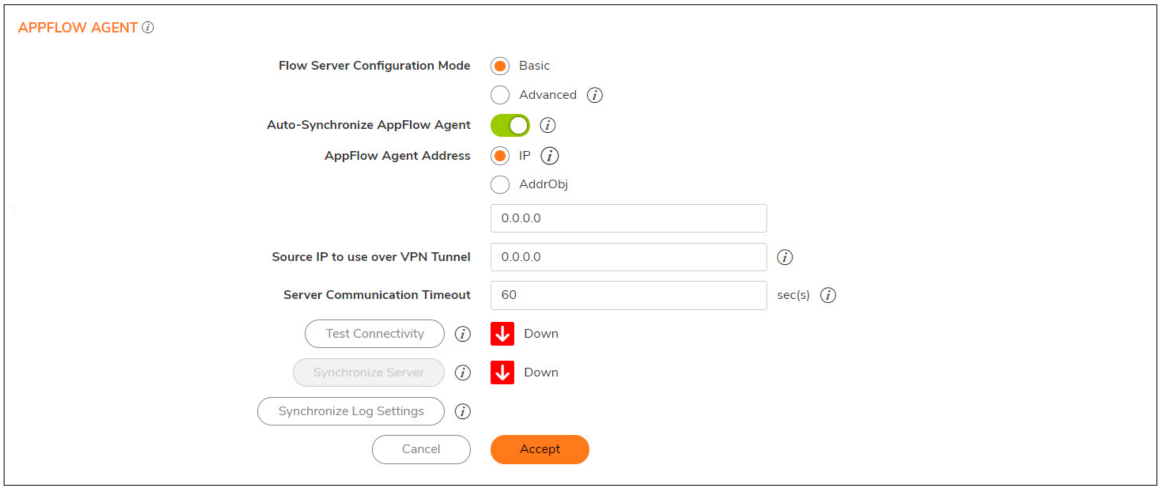
Server Communication Timeout: 60 sec(s)

2. For **Flow Server Configuration Mode**, select either **Basic** or **Advanced** modes. When **Advanced** is selected, additional **Advanced Configuration** options become available to configure alternate flow server and advanced flow settings.
3. For **Auto-Synchronize AppFlow Agent**, the AppFlow Agent needs static data from the firewall before it can display it on the AppFlow Monitor, AppFlow Report, and AppFlow Dashboard. By enabling this checkbox, the firewall automatically synchronizes data to the AppFlow Agent.
4. For **Advanced Flow Server Config Mode**, using **Active Standby** mode, flows are directed to AppFlow Agent 1 (when AppFlow Agent 1 is Up). When AppFlow Agent 1 is Down, and when AppFlow Agent 2 is Up, then the flows are directed to AppFlow Agent 2. In **Load Balancing** mode, you are able to select between **Load Balancing Modes**; **Mirror** and **Share-Load**. These radio buttons are enabled only when **Load Balancing** mode is selected. When **Share-Load** is selected and both flow servers are **Up**, the flows are divided equally amongst the two AppFlow Agent. When mirroring is selected, all the flows are sent to both the flow servers.

5. Under the **AppFlow Agent 1** and **AppFlow Agent 2**, the **AppFlow Agent Address** option **IP**, the device sends AppFlows and real-time data to the specified IP address/address object. If AppFlow Agent is reachable through a VPN tunnel, then you can specify the source IP to use for the VPN tunnel. Note that the address object can only be of type **Host** or **FQDN**.
6. For the **Source IP to use over VPN Tunnel** option, when the AppFlow Agent is reachable through the VPN tunnel, you can specify that IP here. Choose an IP from the VPN policy.
7. Use **Server Communication Timeout** to redirect data to the Dashboard. From the SonicWall firewall GUI, Dashboard data can be pulled from the AppFlow Agent. A Timeout specified is a number of seconds to wait before failing when the data has been fetched from the AppFlow Agent. The minimum value is 60, maximum value is 120 and default value is 60.
8. **Test Connectivity** connects to the AppFlow Agent and gathers registration information, image versions, and counters.
9. Static data can be sent manually to the AppFlow Agent using the **Synchronize Server** option. This can only be done one time after starting of the AppFlow Agent and registering with the firewall.
10. **Synchronize Log Settings** sends the necessary fields of log settings to the AppFlow Agent for log display.

Connecting to an AppFlow Agent

The **DEVICE | AppFlow > AppFlow Agent** page enables you to establish a connection to a AppFlow Agent.



APPFLOW AGENT ⓘ

Flow Server Configuration Mode	● Basic ○ Advanced ⓘ
Auto-Synchronize AppFlow Agent	● ⓘ
AppFlow Agent 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 ⓘ	↓ Down
Synchronize Log Settings ⓘ	
Cancel	Accept

The AppFlow Agent role can be used in a distributed deployment. In this role, the AppFlow Agent 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 an AppFlow Agent in deployment, 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 AppFlow Agent has a fixed Syslog Facility (Local Use 0), Syslog Format (Default), and Server ID (firewall). Although the Event Profile value for the AppFlow Agent is set to 0 by default, all events are reported to your AppFlow Agent regardless of the profile. The AppFlow Agent is also exempted from Rate Limiting. AppFlow Agents can be enabled/disabled only in the Advanced Management section of the **DEVICE | AppFlow > Flow Reporting | Settings** page and not in the **DEVICE | Log > Syslog** page.

Topics:

- Basic Mode
- Advanced Mode

Basic Mode

Establishing a connection is a two-step process:

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

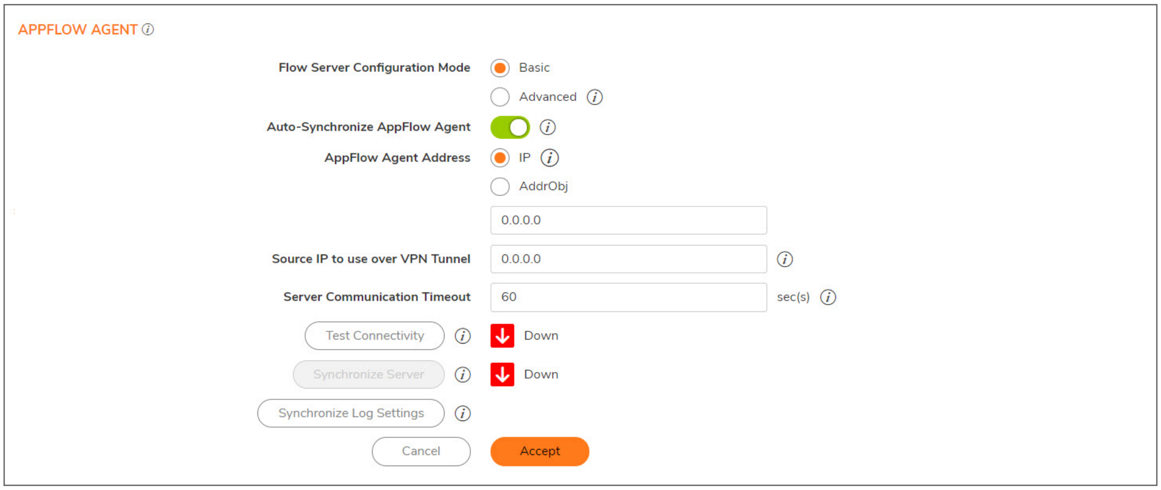
For more detailed information about configuring an AppFlow Agent with GMS, refer to the latest SonicWall GMS or SonicWall Management Services administration documentation, available at https://www.sonicwall.com/support/technical-documentation.

To establish a connection to an AppFlow Agent:

1. Log in to the Instant AppFlow Agent.
2. Go to the **NETWORK | System > Interfaces** page.
3. Find and copy the Host IP address of the AppFlow Agent

On the SonicWall network security appliance:

1. Navigate to the **DEVICE | AppFlow > AppFlow Agent** page.
2. For the **Flow Server Configuration Mode**, **Basic** should be selected. (This is the default setting.)



APPFLOW AGENT

Flow Server Configuration Mode ● Basic ○ Advanced

Auto-Synchronize AppFlow Agent: On

AppFlow Agent 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: Down

3. In the **AppFlow Agent Address** field, either:
   - Paste the Host IP address you copied from the AppFlow Agent.
   - 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**.
4. In the **Source IP to Use over VPN Tunnel** field, specify the source IP address for the applicable VPN policy.

   ⓘ **IMPORTANT:** If the AppFlow Agent 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 AppFlow Agent, click **Test Connectivity**. The connectivity status is displayed.
8. If you want to manually send static data to the AppFlow Agent, 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 AppFlow Agent.
9. Click **Accept**.

Topics:

- Connecting to an AppFlow Agent
- Advanced Mode

Advanced Mode

Advanced Configuration mode allows to specify select more than one AppFlow Agent 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 AppFlow Agent.
2. Configure the AppFlow Agent on the **DEVICE | AppFlow > Flow Reporting** page.

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

To establish a connection to a AppFlow Agent:

1. In GMS, log in to the Instant AppFlow Agentr.
2. Go to the **Network > Settings** page.
3. Find and copy the Host IP address of the AppFlow Agent.

On the SonicWall network security appliance:

1. Navigate to the **DEVICE | AppFlow > AppFlow Agent** page.
2. For the **Flow Server Configuration Mode**, choose **Advanced**.
3. Set the **Advanced Flow Server Config Mode**.
   - **ActiveStandby** — If you select this option, flows are directed first to AppFlow Agent 1 (if available). If AppFlow Agent 1 is not available, flows are directed to the AppFlow Agent 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 **AppFlow Agent Address** fields, either:
   - Paste the Host IP address you copied from the AppFlow Agent.
   - 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**.
5. In the **Source IP to Use for Collector on a VPN Tunnel** field for each AppFlow Agent, specify the source IP address for the applicable VPN policy.

   ⓘ **IMPORTANT:** If the AppFlow Agent 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 AppFlow Agent, 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 AppFlow Agent.
8. To test your connection to a AppFlow Agent, click **Test Connectivity** for that AppFlow Agent. The connectivity status is displayed.
9. If you want to manually send static data to an AppFlow Agent, click **Synchronize Server** for that AppFlow Agent. 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 an AppFlow Agent
- Basic Mode

3

SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- 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

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

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

ⓘ | **TIP:** A TIP icon indicates helpful information.

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

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

SonicOS and SonicOSX Device AppFlow Administration Guide
Updated - July 2021
Software Version - 7
232-005325-00 Rev C

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

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

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

> General Public License Source Code Request
> Attn: Jennifer Anderson
> 1033 McCarthy Blvd
> Milpitas, CA 95035