SonicWall® Management Services System AppFlow

Administration

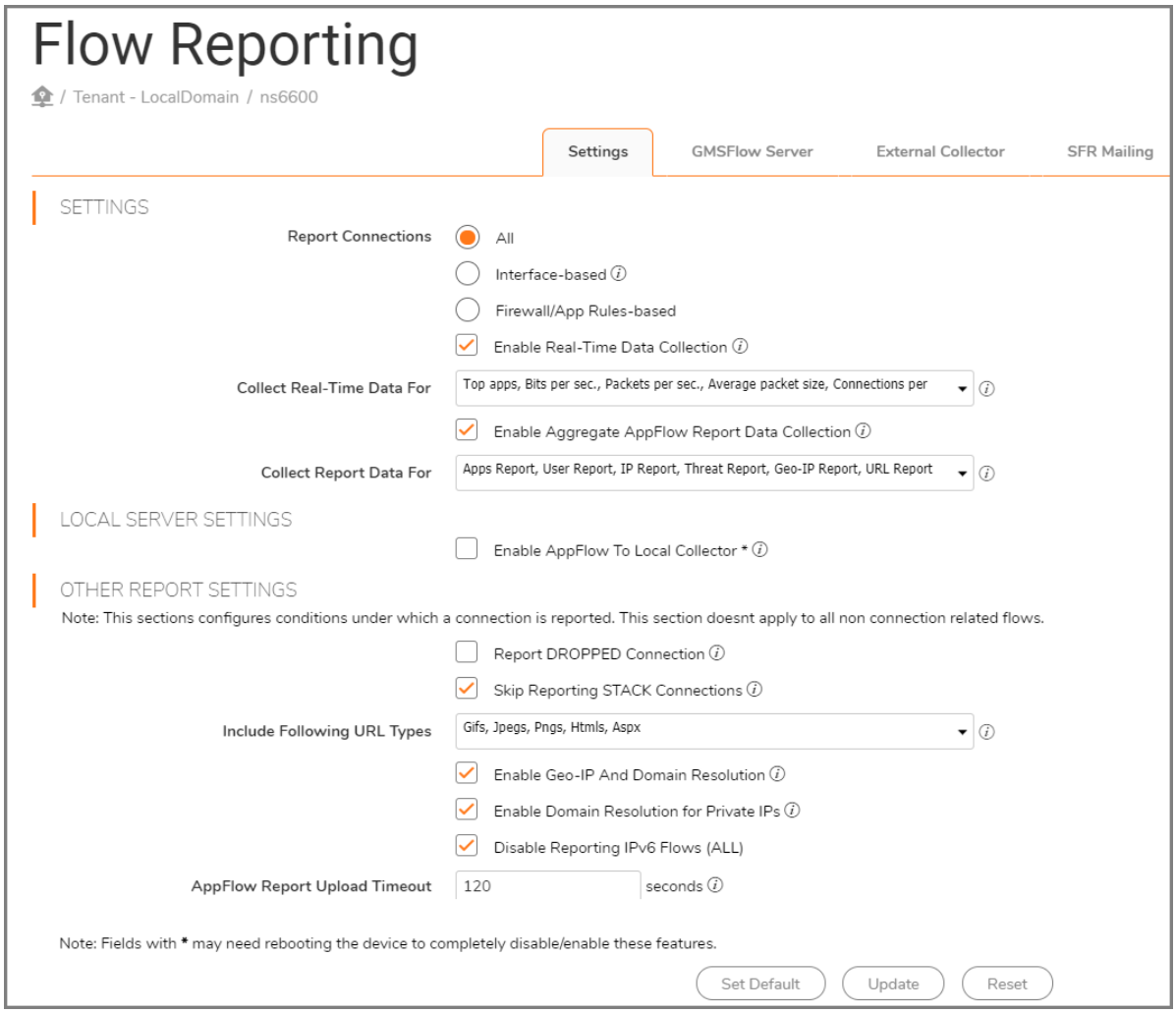
SONICWALL®

Contents

1

Configuring Flow Reporting

The **AppFlow > Flow Reporting** page includes settings for configuring the firewall to view statistics based on Flow Reporting and Internal Reporting. From this screen, you can also configure settings for internal reporting and flow server reporting.

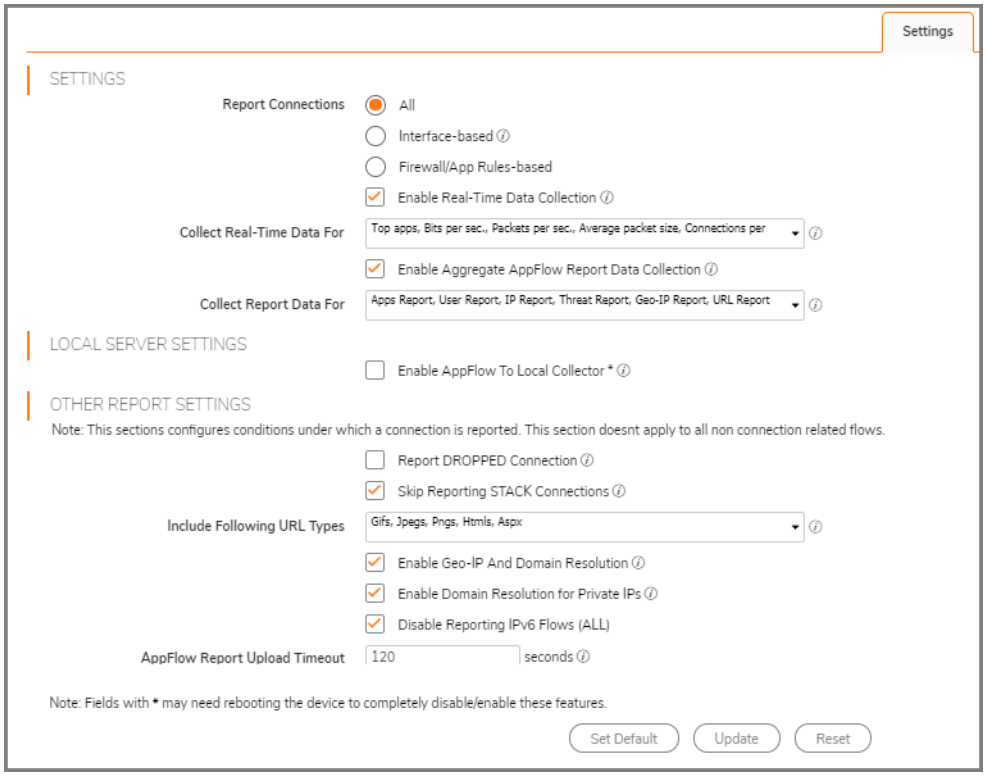


This page includes the following sub-sections arranged as tabs:

- Settings Tab
- GMSFlow Server Tab
- AppsFlow Server
- External Collector Tab
- SFR Mailing Tab

Settings Tab

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

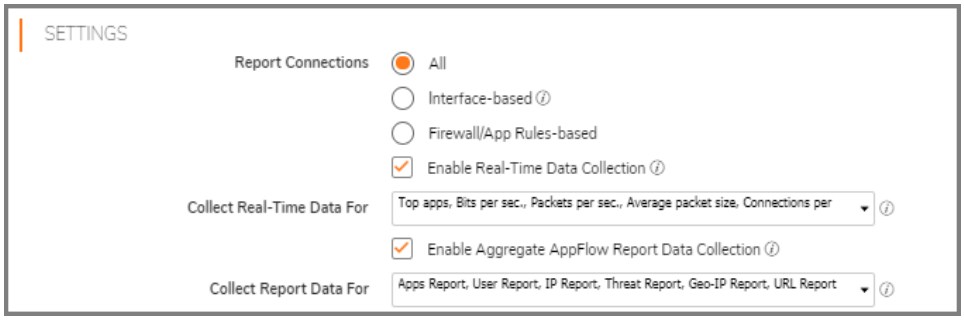


The Settings tab has three sections:

- Settings
- Local Server Settings
- Other Report Settings

Settings

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



- **Report Collections**—Enables AppFlow reporting collection according to one of these modes:
  - **All** — Selecting this check box reports all flows. This is the default setting.
  - **Interface-based** — Selecting this check box enables flow reporting based only on the initiator or responder interface. Only connections from selected interfaces are reported to the appflow collector. 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 **Network > Interfaces** and then click on the pencil icon for edit and be sure **Enable Flow Reporting** is checked. The per interface setting defaults to enabled.

    If an interface has its flow reporting disabled, then flows associated with that interface are skipped.
  - **Firewall/App Rules-based** — Selecting this check box enables flow reporting based on already existing firewall Access and App rules configuration, located on the **Firewall > Access Rules** page (click on the pencil edit icon and then go to **Action** and locate **Enable Flow Reporting**) and the **Firewall > App Rules** (go to edit App Rule) 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 check box to enable flow reporting. If a flow matching a rule is to be reported, this enabled check box forces verification that firewall rules have flow reporting enabled or not.
- **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. The real-time graphs displayed in the **REPORTS > Live Reports** page are disabled.
- **Collect Real-Time Data For** — Select from this pull-down menu the streaming-graphs to display on the Real-Time Monitor page:
  - Top Apps—Displays the **Applications** graph.
  - Bits per second—Displays the **Bandwidth** graph.
  - Packets per second—Displays the **Packet Rate** graph.
  - Average packet size—Displays the **Packet Size** graph.
  - Connections per second—Displays the **Connection Rate** and **Connection Count** graphs.
  - Core utility—Displays the **Multi-Core Monitor** graph.

- **Enable Aggregate AppFlow Report Data Collection** — Enables individual AppFlow Reports collection on your SonicWall appliance for display in **Dashboard > 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 **AppFlow Reports** page by clicking **Display icon by the Enable Aggregate AppFlow Report Data Collection**.

  - **Collect Report Data For** — Select from this drop-down menu the data to display on the **Dashboard > Appflow Reports** page. By default, all reports are selected.
    - **Apps Report**
    - **User Report**
    - **IP Report**
    - **Threat Report**
    - **Geo-IP Report**

Local Server Settings

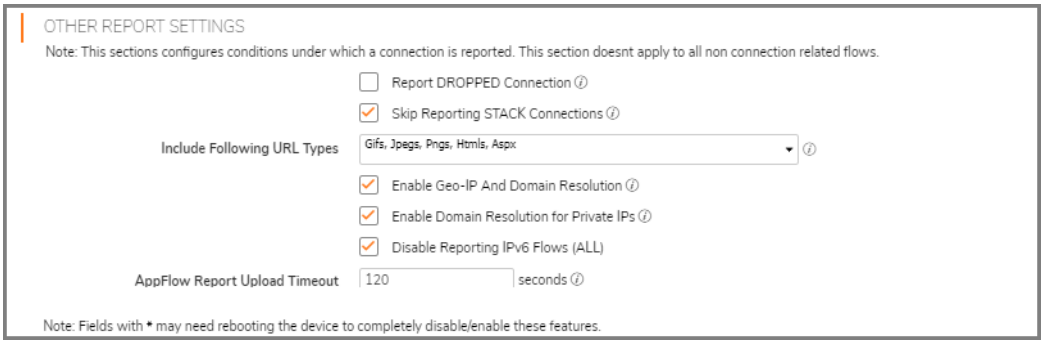
The **Local Server Settings** section allows you to enable AppFlow reporting to an internal collector.

- **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 **Dashboard > AppFlow Monitor** (???same as Access Points > Dashboard) real-time client monitor) are disabled. By default, this option is disabled.

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

Other Report Settings

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



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

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

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

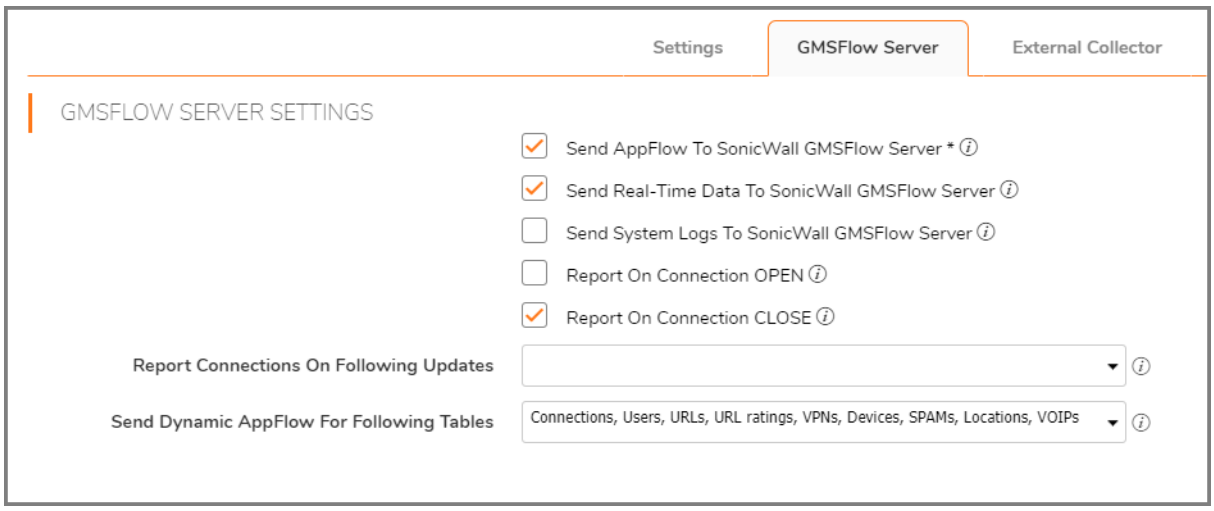
- **Enable Geo-IP Resolution** — Enables Geo-IP resolution. If disabled, the AppFlow Monitor does not group flows based on country under **Initiators** and **Responders** tabs. This setting is unchecked (disabled) by default.

  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 Tab

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



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

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

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

- **Send Real-Time Data to SonicWall GMSFlow Server** —The SonicWall appliance sends real-time data via IPFIX to the SonicWall GMSFlow server. This option is disabled by default.

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

- **Send System Logs to SonicWall GMSFlow Server** — The SonicWall firewall sends system logs via IPFIX to the SonicWall GMSFlow server. This option is not selected by default.
- **Report on Connection OPEN** — The SonicWall appliance reports when a new connection is opened. All associated data related to that connection may not be available when the connection is opened. This option enables flows to show up on the GMSFlow server as soon as a new connection is opened. This option is disabled by default.
- **Report on Connection CLOSE** — The SonicWall appliance reports when a new connection is closed. This is the most efficient way of reporting flows to the GMSFlow server. All associated data related to that connection are available and reported. This option is enabled by default.
- **Report Connections on Following Updates** – The firewall reports when a specified update occurs. Select the updates from the drop-down menu. By default, no update is selected.

threat detection	**VPN tunnel detection**
application detection	**URL detection**
user detection	

IMPORTANT: Connections can still be reported to the GMSFlow server for the following additional triggers. Enabling additional triggers does not affect internal reporting. Flows can still get all additional info like VPN/threat/user info on CLOSE event. The guarantees that this additional info is reported immediately instead of waiting for the connection to CLOSE.

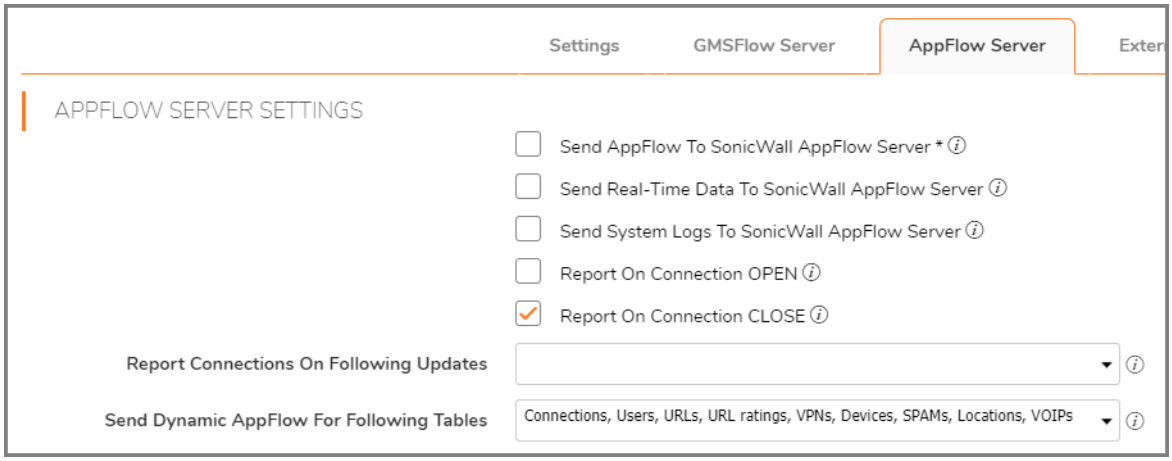
- **Send Dynamic AppFlow For Following Tables** – The firewall sends data for the selected tables. By default, all the tables are selected.

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

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 may create failure when correlating flows with other, related data.

AppsFlow Server

This section provides the network administrator the ability to start sending AppFlow and Real-Time data to an external SonicWall AppFlow Server.



- **Send AppFlow To SonicWall AppFlow Server**— This setting allows you to start sending AppFlow records to an external AppFlow Server. Defaults to enabled.

  If enabled, the SonicWall appliance will send AppFlows data via IPFIX to SonicWall AppFlow server. If disabled, SonicWall App Flow Server will fail to show AppFlow monitor, AppFlow report and AppFlow dashboard chart on AppFlow server or via redirection on a SonicWall device.

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

- **Send Real-Time Data To SonicWall AppFlow Server**— This setting allows you to start sending real-time records to an external AppFlow Server. Defaults to enabled.

If enabled, SonicWall firewall will send real-time data via IPFIX to SonicWall AppFlow server. If disabled, SonicWall AppFlow Server will fail to show real-time chart on AppFlow server or via redirection on SonicWall device.

- **Send System Logs To SonicWall AppFlow Server**— The SonicWall firewall sends system logs via IPFIX to the SonicWall AppFlow server. This option is not selected by default.
- **Report on Connection OPEN**— The SonicWall appliance reports when a new connection is opened. All associated data related to that connection may not be available when the connection is opened. This option enables flows to show up on the AppFlow 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 AppFlow 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. Enabling additional triggers does not affect internal reporting. Flows can still get all additional info like VPN/threat/user info on a CLOSE event. This guarantees this data is reported immediately instead of waiting for close event.

  Threat detection

  Application detection

  User detection

  VPN tunnel detection

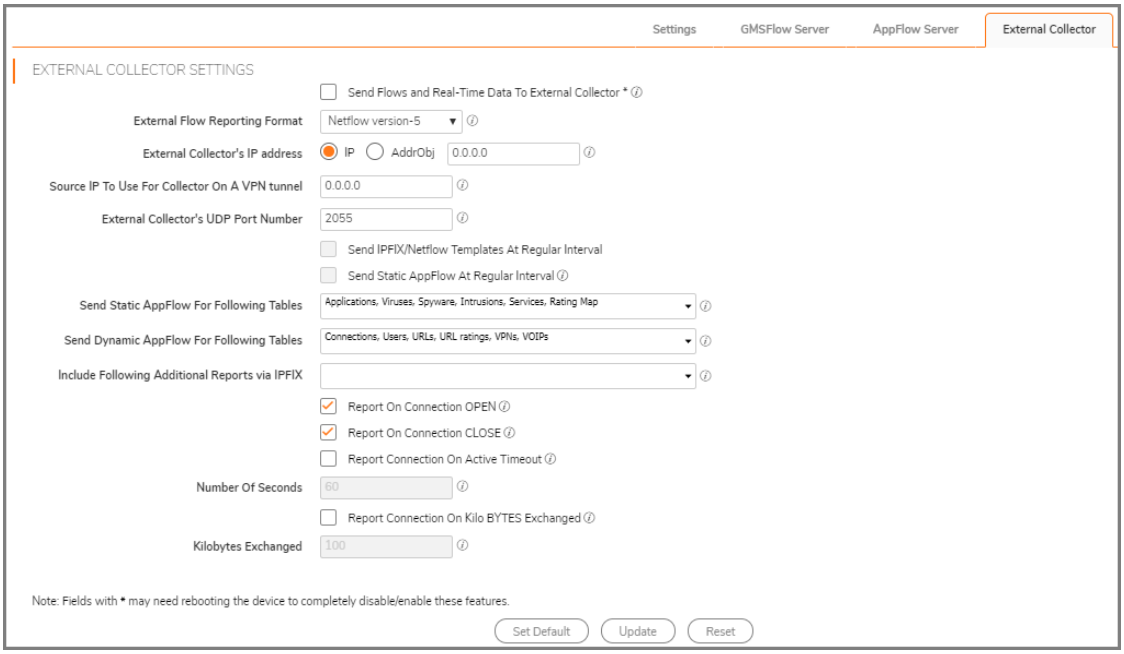
- **Send Dynamic AppFlow For Following Tables** – The firewall sends data for the selected tables. By default, all the tables are selected.

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

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

External Collector Tab

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



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

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

- **External AppFlow Reporting Format**—If the **Report to EXTERNAL Flow Collector** option is selected, you must select the flow-reporting type from the drop-down menu.

NetFlow version-5 (default)	**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, which uses standard data types as defined in IETF. **Netflow** versions and **IPFIX** reporting types contain only connection-related flow details per the standard.
- **IPFIX with extensions**, then only collectors that are SonicWall-flow aware can be used to report SonicWall dynamic tables for:

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

Records reported in IPFIX/Netflow contain connection (flow) details only. IPFIX with extension reports SonicWall dynamic tables for connections, users, applications, threats (Viruses/spyware/intrusion), URLs, logs, real-time health (memory/CPU/interface stats), VPN tunnels, devices, SRAMs, wireless devices and locations.

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

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

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

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

- **External Collector's UDP Port Number**—Specify the UDP port number that Netflow/IPFIX packets are being sent over. The default port is **2055**.
- **Send IPFIX/Netflow Templates at Regular Intervals**—Enables the appliance to send Template flows at regular intervals. This option is selected by default.

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

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

- **Send Static AppFlow at Regular Interval**—Enables the hourly sending of IPFIX records for the specified static appflow 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 in *NEW PUBLICATON*.

  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. In order to generate this, please select needed mapping tables and click generate static flows. If generation of static flows at a periodic interval is selected, then only selected flows will be generated.

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

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

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

  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 may not be available when the connection is opened. This option, however, enables flows to show up on the external collector as soon as the new connection is established. By default, this setting is enabled.
- **Report On Connection CLOSE**—Reports flows when a connection is closed. This is the most efficient way of reporting flows to an external collector. All associated data related to that connection are available and reported. By default, this setting is enabled.
- **Report Connection On Active Timeout**—Reports connections based on Active Timeout sessions. If enabled, the firewall reports an active connection every active timeout period. By default, this setting is disabled.

  NOTE: If you select this option, the **Report Connection On Kilo BYTES Exchanged** option cannot be selected also.

  - **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.

  - **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.

SFR Mailing Tab

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

- SFR Email Settings
- Scheduling SFR Reports by Email
- Deleting Scheduled Reports

SFR Email Settings

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

1 Navigate to **System | Appflow Settings > Flow Reporting**.

2 Click the **SFR Mailing** tab.

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

4 Enter these options:

- The address of the email server in the **SMTP Server Host Name** field.
- The recipient's email address in the **E-mail To** field.
- The email address used for the sender in the **From E-mail** field.
- The SMTP port number in the **SMTP Port** field. The default value is **25**.
- A security method for the email from the **Connection Security Method** drop-down menu:
  - **None** (default)
  - **SSL/TLS**
  - **STARTTLS**

5 If your email server requires SMTP authentication, select the **Enable SMTP Authentication** checkbox and enter these options:

- User name in the **SMTP User Name** field
- Password in the **SMTP User Password** field

6 If your email server supports POP Before SMTP authentication, you can select the **POP Before SMTP** checkbox and enter these options:

- Address of the POP server in the **POP Server Address** field.
- User name in the **POP User Name** field
- Password in the **POP User Password** field.

7 Click **Update**.

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:

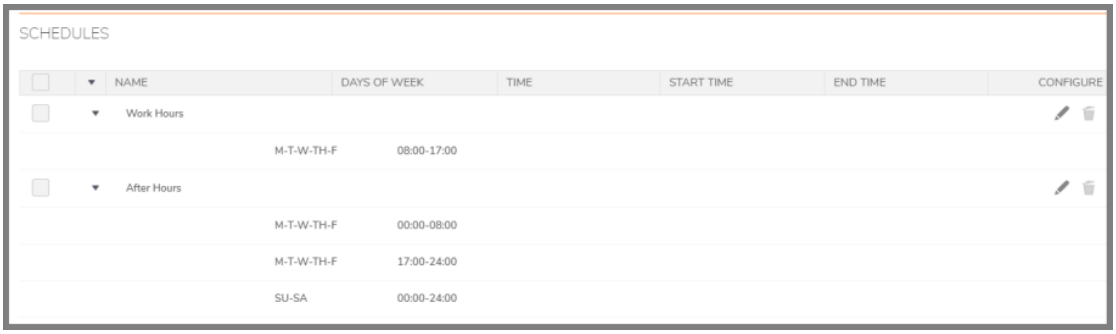
1 Navigate to **System | Appflow Settings > Flow Reporting**.

2 Click the **SFR Mailing** tab.

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

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

5 The Add Schedule dialog box appears.



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

7 Select how often you want the report sent:

- **Once** – Send the report one time at the specified date and time.
- **Recurring** – Send the report on a recurring basis on the specified days and time.
- **Mixed** – Send the report one time and on a recurring basis on the specified days and time.

Topics:

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

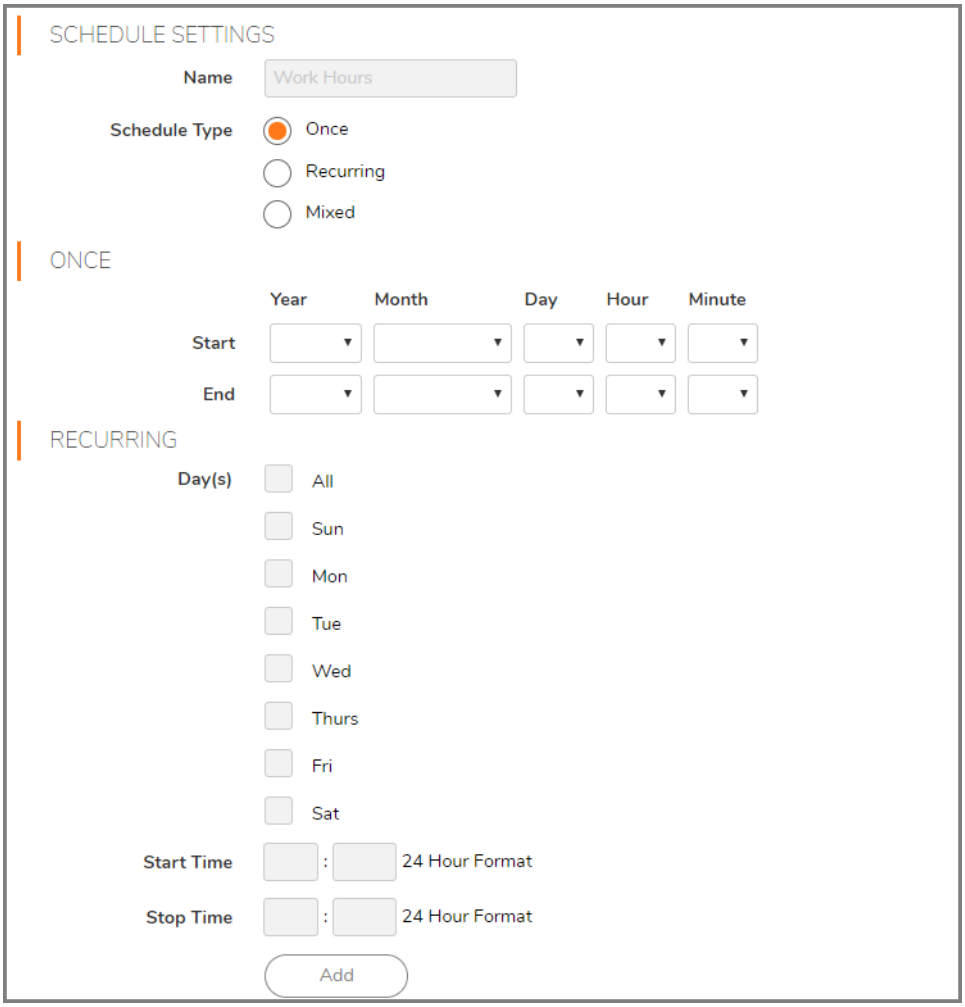
Scheduling One-Time Delivery of the SFR

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

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

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

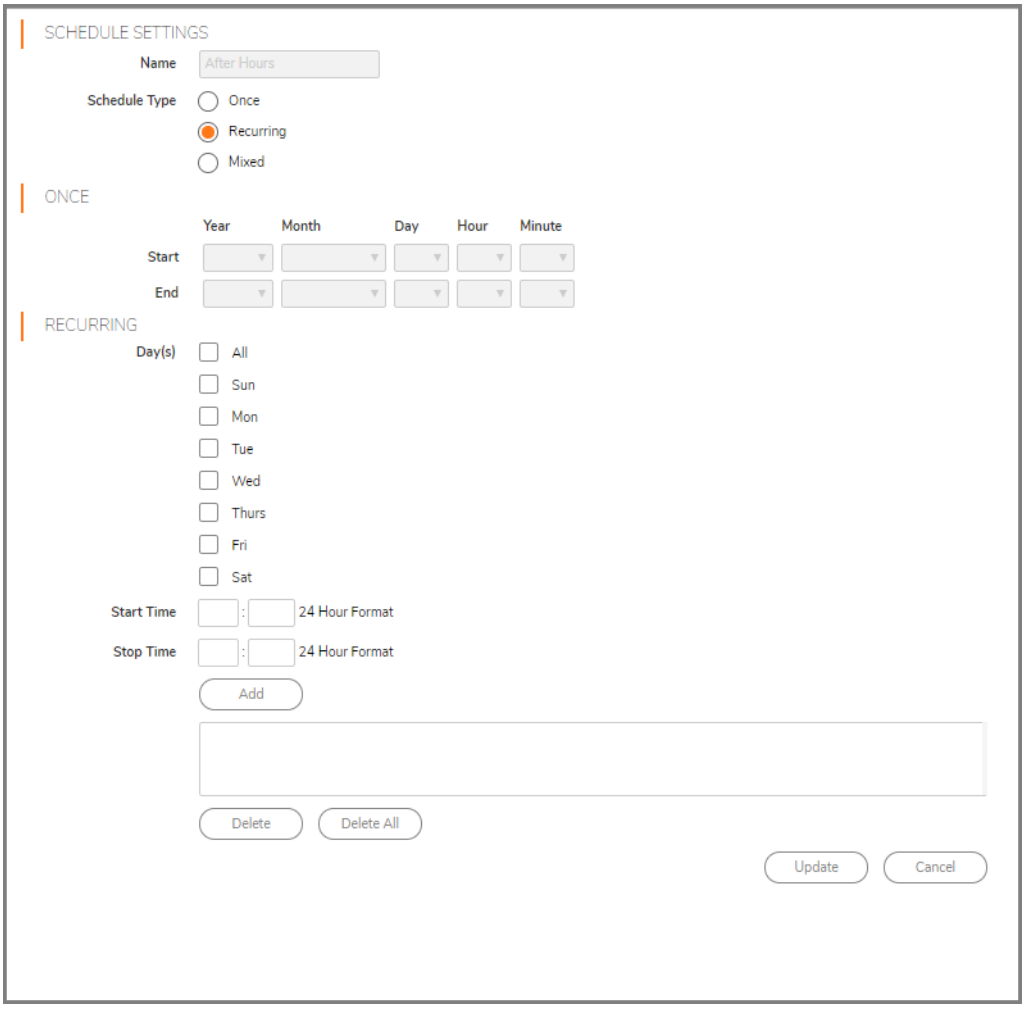
3 Click **OK**.



Scheduling Recurring Delivery of the SFR

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

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



a In the **Recurring** section: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.

2 Click **OK**.

Deleting Scheduled Reports

You can delete any or all scheduled reports.

To delete selected scheduled reports:

1 Select the reports to be deleted in the **Schedule List**.

2 Click **Delete**. The reports you selected will be deleted from the list.

3 Click **OK**.

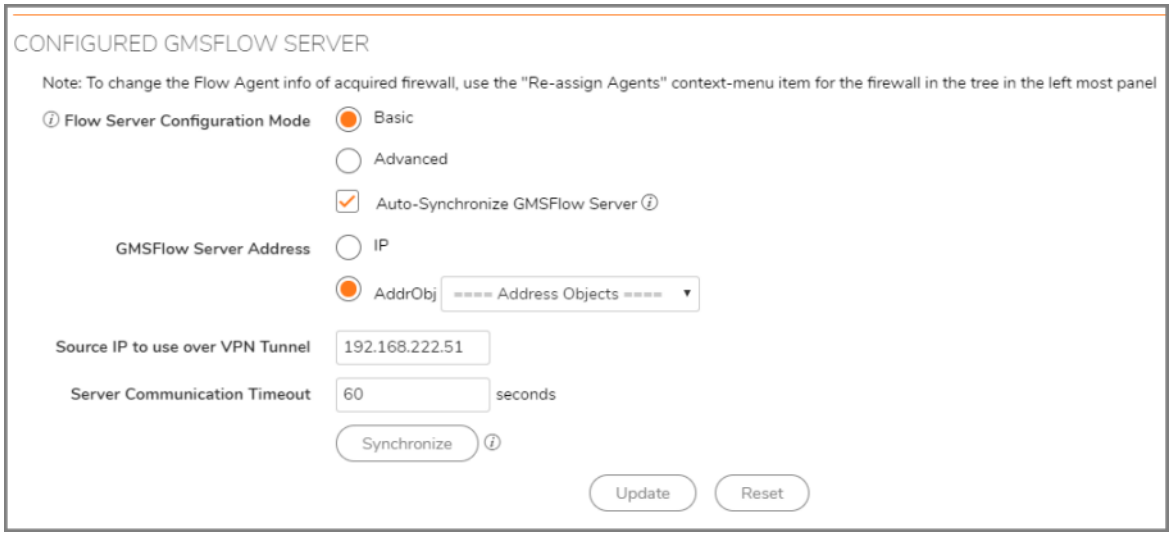
To delete all scheduled reports:

1 Click **Delete All**. All of the reports will be deleted from the list.

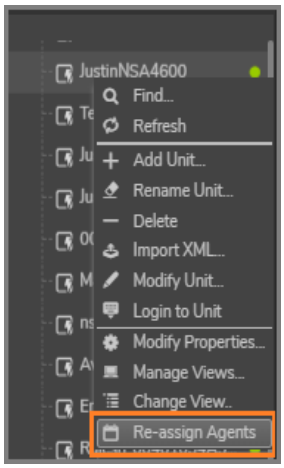
2 Click **OK**.

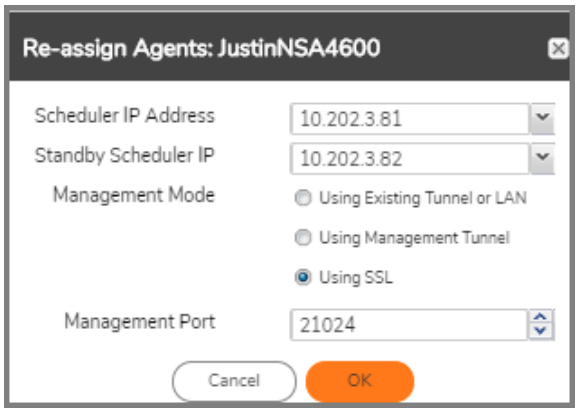
Configuring GMSFlow Server Settings

This page supports setup of a GMSFlow server.



NOTE: To change the Flow Agent info of acquired firewall, use the "Re-assign Agents" context-menu item for the firewall in the tree in the left most panel.

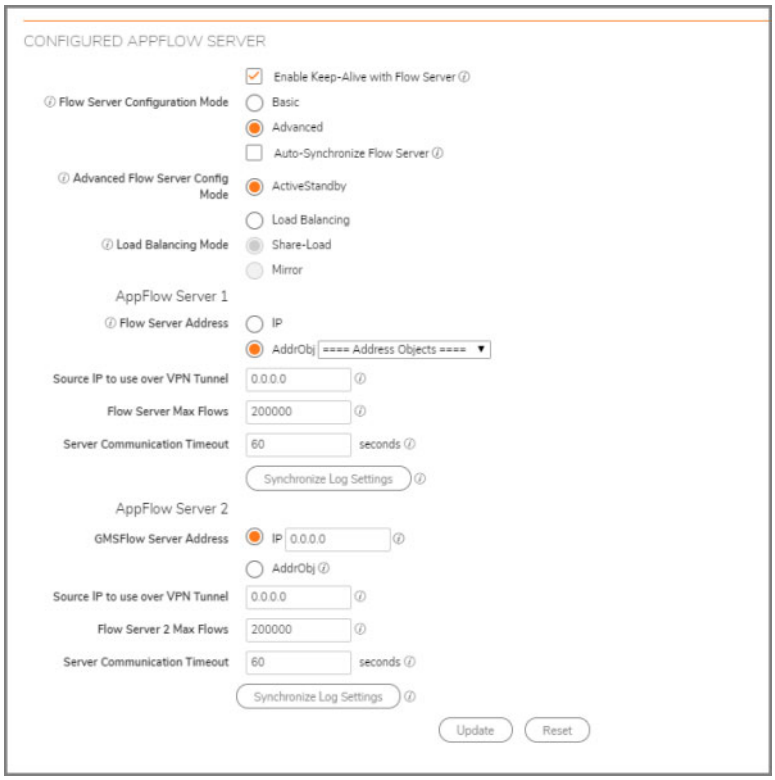




- **Flow Server Configuration Mode** — Basic or Advanced. When Advanced is selected, an alternative flow server and advanced settings may be selected. Not all SonicWall appliances will support Advanced Configuration.
- **Auto-Synchronize GMSFlow Server** — GMSFlow server needs static data from the firewall before it can display AppFlow Monitor, AppFlow Report, and AppFlow Dashboard. By enabling this checkbox, the firewall automatically syncs this data to the GMSFlow server.

- **GMSFlow Server Address** — Supported as IP address or address object. SonicWall device will send AppFlows and real-time data to the specified IP address / address object. If AppFlow sever is readable via VPN tunnel then please specify the source IP to use for VPN tunnel in the following entry field. Note that the address object can only be of the type Host or FQDN.
- **Source IP to use over VPN tunnel** — Defines source of tunneled flow from the source SonicWall appliance. The address object can only be of the type Host or FQDN.
- **Server Communication Timeout —** Set the minimum acceptable time for no response.
- **Synchronize** — Sends the necessary fields of log settings to GMSFlow server for display.

Additional settings are available in Advanced Configuration mode.

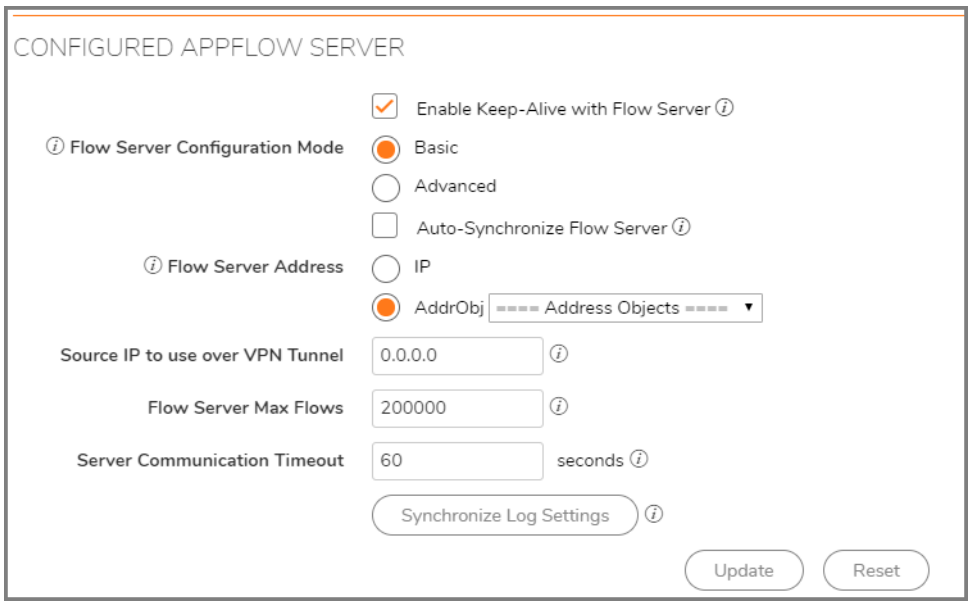


- **Advanced Flow Server Config Mode** — This allows dual GMSFlow servers to be configured for **Active Standby** or **Load Sharing**.
- **Advanced Flow Server Configuration —** In **Active Standby** mode, flows shall be directed to the Flow Server1 (if Flow Server1 is UP). When Flow Server1 is Down, and if Flow Server 2 is UP, then flows shall be directed to Flow Server2. In **Load Balancing** mode, the users can select between mirroring and shared-load operation.
- **Load Balancing Mode —** The radio buttons will only be enabled if **Share -Load** mode is selected. If Share-Load is selected and both flow servers are Up, the flows should be divided equally between the two flow servers. If **Mirror** is selected all the flows will be sent to both of the flow servers.

3

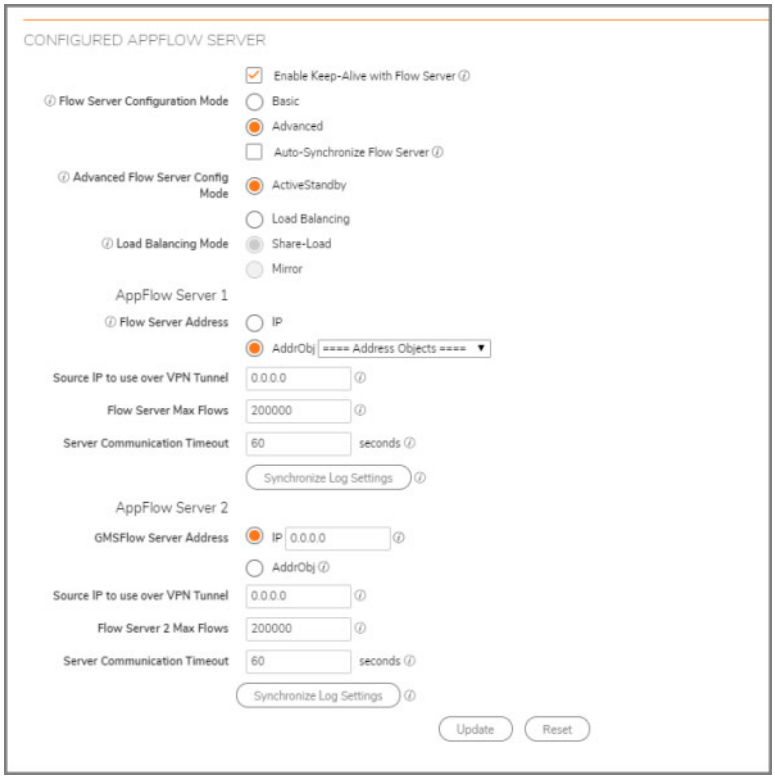
Configuring AppFlow Server Settings

The AppFlow Servers page (**MANAGE | AppFlow > AppFlow Server**) identifies the AppFlow server for a specific Sonic Wall Appliance. Network administrators can configure a central AppFlow Server to support multiple firewalls.



- **Flow Server Configuration Mode** — **Basic** or **Advanced**. When Advanced is selected, an alternative flow server and advanced settings may be selected.
- Auto-Synchronize GMSFlow Server — GMSFlow server needs static data from the firewall before it can display AppFlow Monitor, AppFlow Report, and AppFlow dashboard. By enabling this checkbox, the firewall automatically syncs this data to the GMSFlow server.
- **GMSFlow Server Address** — Supported as IP address or address object. SonicWall device will send AppFlows and real-time data to the specified IP address / address object. If GMSFlow sever is readable via VPN tunnel then please specify the source IP to use for VPN tunnel in the following entry field. Note that the address object can only be of the type Host or FQDN.
- **Source IP to use over VPN tunnel** — Defines source of tunneled flow from the source SonicWall appliance. The address object can only be of the type Host or FQDN.
- **Server Communication Timeout —** Set the minimum acceptable time for no response.
- **Synchronize** — Sends the necessary fields of log settings to GMSFlow server.

Additional settings are available in Advanced Configuration mode.



- **Advanced Flow Server Config Mode** — This allows dual AppFlow servers to be configured for **Active Standby** or **Load Sharing**.
- **Advanced Flow Server Configuration —** In **Active Standby** mode, flows shall be directed to the Flow Server1 (if Flow Server1 is UP). When Flow Server1 is Down, and if Flow Server 2 is UP, then flows shall be directed to Flow Server2. In **Load Balancing** mode, the users can select between mirroring and shared-load operation.
- **Load Balancing Mode —** The radio buttons will only be enabled if **Share -Load** mode is selected. If Share-Load is selected and both flow servers are Up, the flows should be divided equally between the two flow servers. If **Mirror** is selected all the flows will be sent to both of the flow servers.

4

NetFlow Tables

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

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

Exportable Dynamic IPFIX Tables

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

Templates

The following section shows examples of the type of Netflow template tables that are exported. You can perform a Diagnostic Report of your own Netflow Configuration by navigating to **Diagnostics > Network**, and clicking the **Fetch Tech Support Report** button in the **Tech Support Report** section.

Topics:

NetFlow Version 5

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

NetFlow Version 5 Header Format

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)

Netflow Version 5 Record Format (Continued)

Bytes	Contents	Description
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 may 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 may 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 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 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
```

5

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.

Management Services System AppFlow Administration
Updated - November 2018
232-004553-00 Rev A