SonicOS 7.0

Monitor Appflow

Administration Guide

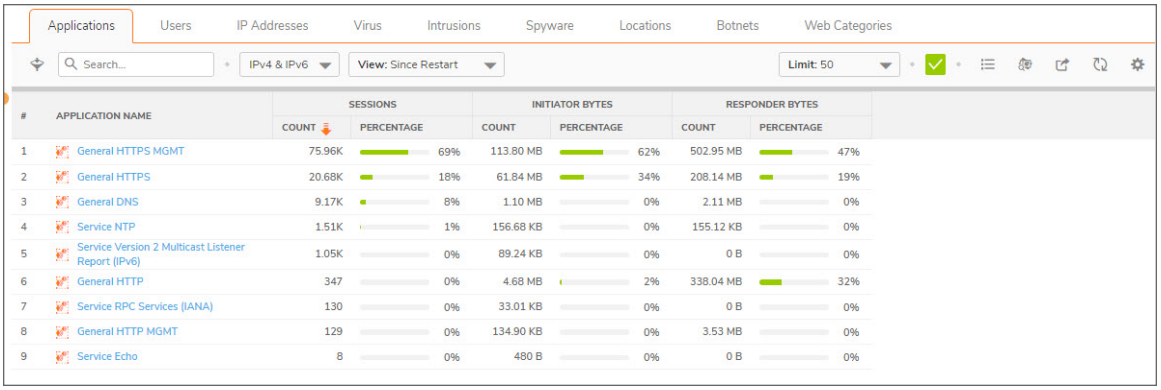
SONICWALL®

Contents

1

AppFlow Report

The **MONITOR | AppFlow > AppFlow Reports** page displays the following reports:



#	APPLICATION NAME	SESSIONS		INITIATOR BYTES		RESPONDER BYTES	
		COUNT	PERCENTAGE	COUNT	PERCENTAGE	COUNT	PERCENTAGE
1	General HTTPS MGMT	75.96K	69%	113.80 MB	62%	502.95 MB	47%
2	General HTTPS	20.68K	18%	61.84 MB	34%	208.14 MB	19%
3	General DNS	9.17K	8%	1.10 MB	0%	2.11 MB	0%
4	Service NTP	1.51K	1%	156.68 KB	0%	155.12 KB	0%
5	Service Version 2 Multicast Listener Report (IPv6)	1.05K	0%	89.24 KB	0%	0 B	0%
6	General HTTP	347	0%	4.68 MB	2%	338.04 MB	32%
7	Service RPC Services (IANA)	130	0%	33.01 KB	0%	0 B	0%
8	General HTTP MGMT	129	0%	134.90 KB	0%	3.53 MB	0%
9	Service Echo	8	0%	480 B	0%	0 B	0%

The **MONITOR | AppFlow > AppFlow Report** page enables you to view top-level aggregate reports of what is going on in your network and, at a quick glance, answer such questions as the following:

- What are the top-most used applications running in my network?
- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?

The report data can be viewed from the point of the last system restart or since the data was last reset.

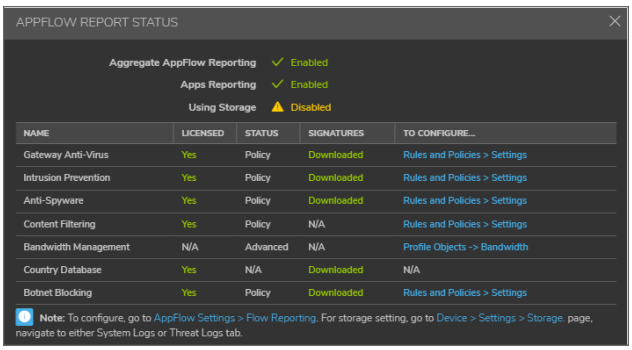
To enable and configure the reports, follow the procedures described in **Managing Flow Reporting Statistics** in the **SonicOS Logs** documentation. The green check mark icon at the top of the **MONITOR | AppFlow > AppFlow Report** page displays a link to the **DEVICE | AppFlow Settings > Flow Reporting** page, where you can configure the reports.

The top of the page displays the following settings and information:

- **IP Version** – Select IPv4, IPv6, or IPv4 and IPv6 to view the reports for that traffic.
- **View** – Choose View type to display reports based on the total activity **Since Restart** of firewall, activity **Since Last Restart** by user of activity based on the configured schedule. If **On Schedule** then you can configure to export report either by way of FTP/e-mail.

  Choose one:

  - **Since Restart** – Shows the aggregate statistics since the last appliance restart.
  - **Since Last Reset** – Shows the aggregate statistics since the last time you cleared the statistics.
  - **On Schedule** – You can configure to export your report either by FTP or e-mail.
- **Limit** – Limits the number of resulting entries.
- **Check mark** – Click or mouse over to expose a popup showing the Appflow Report Status. Links are provided to connect you to additional data.



- **Refresh** – Click to refresh the report data.

Topics:

- Top Applications
- Top Users
- Top IP Addresses
- Top Viruses
- Top Intrusions
- Top Spyware
- Top Locations
- Top Botnets
- Top Web Categories

Applications

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based

on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

When viewing the Applications data, the key information is provided in the table:

- **Sessions** — Number of connections or flows
- **Initiator Bytes** — Number of bytes sent by the initiator
- **Responder Bytes** — Number of bytes sent by the responder

Additionally, the report provides the following information:

- **Application Name** — Name of the application - Signature ID
- **Count** — The frequency of this application in KBs of the total number of applications.
- **Percentage of Applications** — The frequency of this application as a percentage of the total number of applications
- **Access Rules** — Number of connections/flows blocked by the firewall rules
- **App Rules** — Number of connections/flows blocked by DPI engine
- **Location Block** — Number of connections/flows blocked by GEO enforcement
- **Botnet Block** — Number of connections/flows blocked by BOTNET enforcement
- **Virus** — Number of connections/flows with virus
- **Intrusion** — Number of connections/flows identified as intrusions
- **Spyware** — Number of connections/flows with spyware

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Users

Using the **View** drop-down list, select **Since Restart**, **Since Last Reset**, or **On Schedule**.

These selections are defined as:

- **Sessions** — Number of sessions/connections initiated/responded
- **Bytes Received** — Number of bytes received by the user
- **Bytes Sent** — Bytes of data sent by the user

The report provides the following information:

- **User Name** — Name of the user, or UNKNOWN
- **Count** — The activity of this user in KBs of the total activity of users
- **Percentage of Users** — The activity of this user as a percentage of the total activity of users
- **Blocked** — Connections/sessions blocked
- **Virus** — Number of connections/flows with virus

- **Spyware** — Sessions/connections detected with spyware
- **Intrusion** — Number of Sessions/connections identified as intrusions
- **Botnet** — Sessions/Connections detected as botnetThe columns in the table can be customized so it displays only what you want to see.

Click the gear icon to select columns.

IP Addresses

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

When viewing the IP Addresses data, the key information is provided in the table:

- **Sessions** — Number of sessions/connections initiated/responded
- **Bytes Received** — Number of bytes received by the user
- **Bytes Sent** — Bytes of data sent by the user

The report provides the following information:

- **IP Address** — The IP address
- **Count** — The frequency of connections/flows involving this IP address in KBs of the total number of connections/flows for all IP addresses
- **Percentage of IP Addresses** — The frequency of connections/flows involving this IP address as a percentage of the total number of connections/flows for all IP addresses
- **Blocked** — Connections/sessions blocked
- **Virus** — Number of connections/flows with virus
- **Spyware** — Sessions/connections detected with spyware
- **Intrusion** — Number of Sessions/connections identified as intrusions
- **Botnet** — Sessions/Connections detected as botnet

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Viruses

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Sessions** — Number of sessions/connections with this virus

The report provides the following information:

- **Virus Name** — The name of the virus, or UNKNOWN
- **Count** — The frequency of this virus in KBs of the total number of viruses
- **Percentage of Viruses** — The frequency of this virus as a percentage of the total number of viruses

Intrusions

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Sessions** — Number of sessions/connections with this virus

The report provides the following information:

- **Intrusion Name** — The name of the intrusion, or UNKNOWN
- **Count** — The frequency of this intrusion in KBs of the total number of intrusions
- **Percentage of Intrusions** — The frequency of this intrusion as a percentage of the total number of intrusions

Spyware

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

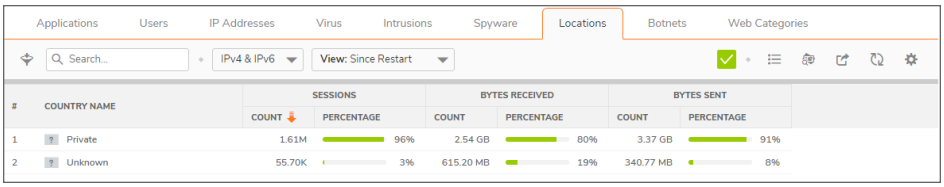
The report provides the following information:

- **Sessions** — Number of sessions/connections with this virus

The report provides the following information:

- **Spyware Name** — The name of the spyware signature, or UNKNOWN
- **Count** — The frequency of this spyware in KBs of the total number of spyware
- **Percentage of Spyware** — The frequency of this spyware as a percentage of the total number of spyware

Locations



Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

These selections are defined as:

- **Sessions** — Number of sessions/connections initiated/responded
- **Bytes Received** — Number of bytes received by the user
- **Bytes Sent** — Bytes of data sent by the user

The report provides the following information:

- **Country Name** — Name of the location or country
- **Count** — The frequency of of connections/flows involving this location in KBs of the total number of connections/flows for all locations
- **Percentage of Locations** — The frequency of connections/flows involving this location as a percentage of the total number of connections/flows for all locations
- **Dropped** — Number of sessions/Connections dropped

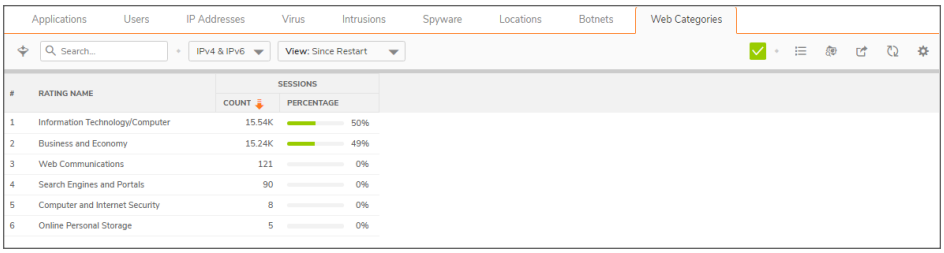
Botnets

Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Botnet Name** — Name of the Botnet
- **Count** — Sessions or connections detected as a botnet

Web Categories



Using the **View** drop-down list, select what you want included in the Applications report. The view type defines reporting based on the total activity **Since Restart** of firewall, activity **Since Last Reset** by user, or activity based on the configured schedule. If you select **On Schedule**, you can configure to export report either via FTP or email.

The report provides the following information:

- **Sessions** — Number of sessions/connections

The report provides the following information:

- **Rating Name** — The name of URL category
- **Count** — The frequency of access to URLs in this rating category in KBs of the total number of URL accesses
- **Percentage of Viruses** — The frequency of access to URLs in this rating category as a percentage of the total number of URL accesses

2

AppFlow Monitor

The **MONITOR | AppFlow > AppFlow Monitor** page displays a series of reports. Select the appropriate tab for one of the reports:

- Top Applications
- Top Users
- Top Web Activity
- Top Initiator IPs
- Top Responder IPs
- Top Threats
- Top VoIP
- Top VPN
- Top Devices
- Top Contents
- Top Policies

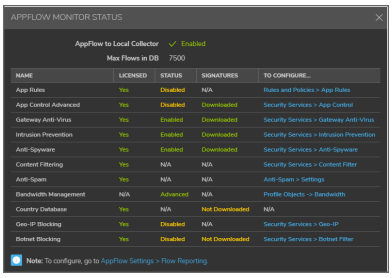
The **MONITOR | AppFlow > AppFlow Monitor** page enables you to monitor top-level aggregate reports of what is going on in your network and, at a quick glance, answer such questions as the following:

- What are the top-most used applications running in my network?
- Which applications in terms of total number of sessions and bytes consume my network bandwidth?
- Which applications have viruses, intrusions, and spyware?
- What website categories are my users visiting?

To enable and configure the reports, follow the procedures described in **Managing Flow Reporting Statistics** in the **SonicOS Logs** documentation. The green check mark icon at the top of the **MONITOR | AppFlow > AppFlow Monitor** page displays a link to the **DEVICE | AppFlow Settings > Flow Reporting** page, where you can configure the reports.

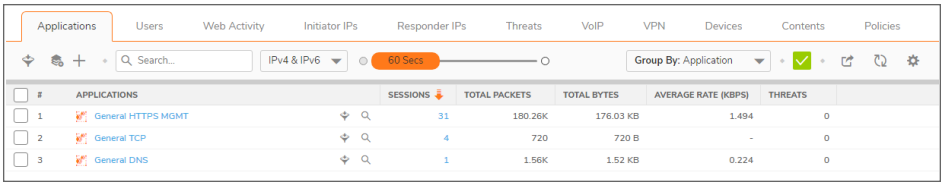
The top of the page displays the following settings and information:

- **+Create** – Click to create filtering on incidents
- **+Add to Filter** – Click to add filter criteria to selected applications
- **IP Version** – Select IPv4, IPv6, or IPv4 and IPv6 to view the reports on that traffic.
- **Slider** – Use the slider to filter flow results as of the Last 60 secs, 2 minutes, 10 minutes, 15 minutes, 30 minutes, 60 minutes, 3 hours, 6 hours, 12 hours, 24 hours, 7 days, 15 days, 30 days, or All Flows
- **Group By** – Filters results by grouping flows based on **Application**, **Category**, or **Signature**
- **Check mark** – Click or mouse over to expose a popup showing the Appflow Monitor Status. Links are provided to connect you to additional data.



- **Refresh** – Click to refresh the report data.

Applications



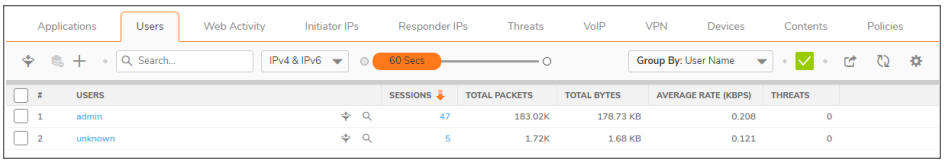
You can filter flows by **Application**. Applications can be grouped by **Application**, **Category**, or **Signature**.

These selections are defined as:

- **Application** — Name of the application - Signature ID
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions or connections identified with intrusions, spyware, or a virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Users



The Users report allows filtering by **Users**. Users can be grouped the following:

- **User** — Name of the user- Signature ID
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Web Activity

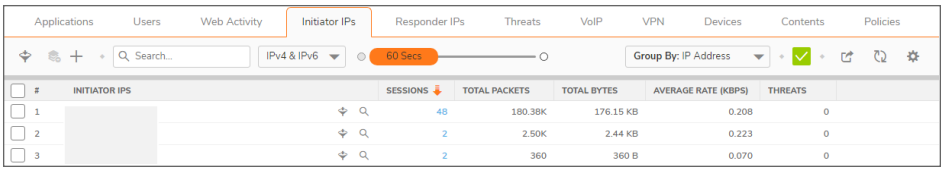
You can filter flows by **Web Activity**. Web URLs can be grouped by **Domain Name**, **URL**, or **Ratings**.

These selections are defined as:

- **Domain Name** — Name of the web domain
- **Add entry to filter** — Icon appears allowing you to add specific domain names into your filtering
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Initiator IPs



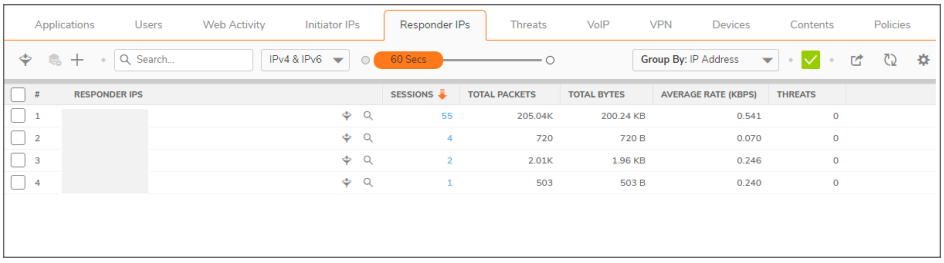
You can filter flows by **Initiator IP**. Initiator IPs can be grouped by **IP Address**, **Interface**, or **Country**.

These selections are defined as:

- **Initiator** — Name of the initiator IP address
- **Add entry to filter** — Icon appears allowing you to add specific initiator IP addresses into your filtering
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Responder IPs



You can filter flows by **Responder IPs**. Responder IPs can be grouped by **IP Address**, **Interface**, or **Country**.

These selections are defined as:

- **Responder** — Name of the responder IP address
- **Add entry to filter** — Icon appears allowing you to add specific responder IP addresses into your filtering
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets

- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Threats

You can filter flows by **Threat**. Threats can be grouped as **All**, **Intrusion**, **Virus**, **Spyware**, **Anti-Spam**, or **Botnet**.

These selections are defined as:

- **Threat** — Name of the threat
- **Add entry to filter** — Icon appears allowing you to add specific threats into your filtering
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

VoIP

You can filter flows by **VoIP**. VoIP can be grouped as **Media Type** or **Caller ID**.

These selections are defined as:

- **VoIP** — Name of the VoIP
- **Sessions** — Number of connections or flows.
- **Total Packets** — Number of packets.
- **Total Bytes** — Number of bytes sent by the initiator.
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections).
- **Out of Sequence/Lost Pkts** — Number of out of sequence or lost packets.
- **Average Jitter (msec)** — The average jitter or time delay between when a signal is transmitted and when it is received. It is measured in milliseconds.

- **Maximum Jitter (msec)** — The maximum amount of jitter between when a signal is transmitted and when it is received, measured in milliseconds.**Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

VPN

You can filter flows by **VPN**. VPN can be grouped by **Remote IP Address**, **Local IP Address**, or **Name**.

These selections are defined as:

- **VPN** — Name of the VPN
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Devices

You can filter flows by **Device** IP address. Devices can be grouped by **IP Address**, **Interface**, **Name**, or **Vendor**.

These selections are defined as:

- **Device** — Name of the device
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Contents

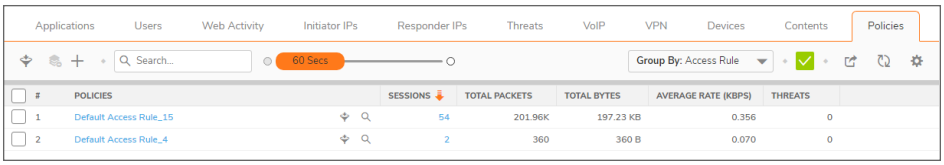
You can filter flows by **Contents**. Content can be grouped by **File Type** or **Email Address**.

These selections are defined as:

- **Content** — Name of the content
- **Sessions** — Number of connections/flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions/spyware/virus.

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

Policies



You can filter flows by **Policies**. Seurity Policies can be grouped by **Access Rule**, **NAT Rule**, **Initiator Route Policy**, or **Responder Route Policy**.

These selections are defined as:

- **Policies** — Name of the security policy to be monitored
- **Sessions** — Number of connections or flows
- **Total Packets** — Number of packets
- **Total Bytes** — Number of bytes sent by the initiator
- **Average Rate (KBPS)** — Current average rate (calculated over the lifetime of connections)
- **Threats** — Number of sessions/connections identified with intrusions, spyware, or a virus

The columns in the table can be customized so it displays only what you want to see. Click the gear icon to select columns.

3

AppFlow Sessions

ⓘ | **NOTE:** Appflow Session are a feature of SonicOS running Policy Mode. It is not available in Classic Mode.

The **MONITOR | AppFlow > AppFlow Sessions** page displays the following reports:

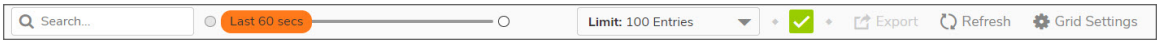
- All
- Threats
- Web Access

The **MONITOR | AppFlow > AppFlow Sessions** page enables you to monitor the status of top-level aggregate reports of what is going on in your network and, at a quick glance, answer such questions as the following:

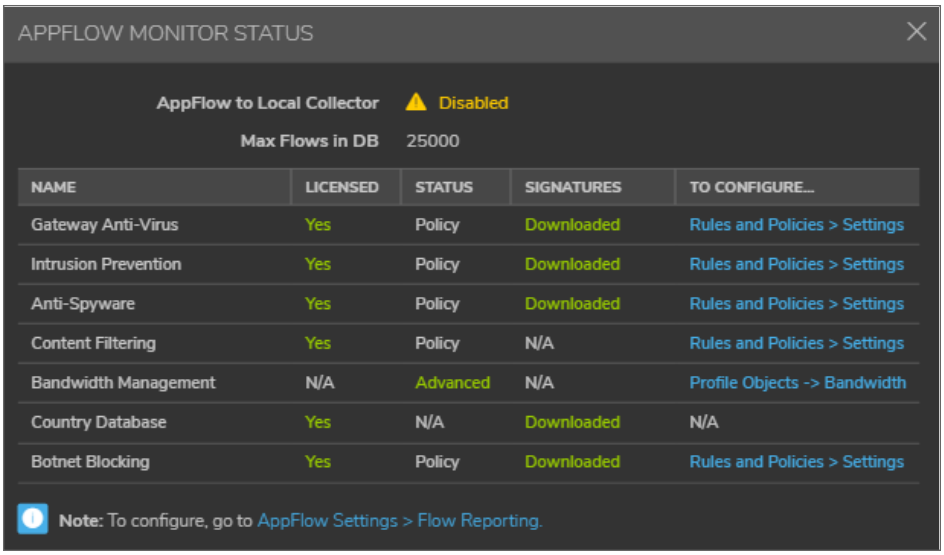
- What are the top-most used applications running in my network?
- Which viruses, intrusions, and spyware have threatened my network?
- What website categories are my users visiting?

To enable and configure the reports, follow the procedures described in **Managing Flow Reporting Statistics** in the **SonicOS Logs** documentation.

The top of the page displays the following settings and information:



- **Slider** – Use the slider to filter flow results as of the Last 60 secs, 2 minutes, 10 minutes, 15 minutes, 30 minutes, 60 minutes, 3 hours, 6 hours, 12 hours, 24 hours, 7 days, 15 days, 30 days, or All Flows
- **Limit** – Limits results by filtering flows based on the number of entries
- **Check mark** – The green check mark icon at the top of the **MONITOR | AppFlow > AppFlow Sessions** page displays a popup showing the Appflow Monitor Status for Policy Mode. Links are provided to connect you to additional data and procedures.



- **Refresh** – Click to refresh the report data.

All

Choose the **All** tab to see all the AppFlow sessions. Application entries can be displayed as either limited or unlimited. Column **Grid Settings** can be added or removed, or expanded and rearranged.

Click **Grid Settings**, and use the arrows next to the column **Name** to expand column options. A checkbox next to a name adds the selection to the grid.

Threats

Select the **Threats** tab to show the monitoring status of AppFlow sessions that contain threats. Entries can be displayed as either limited or unlimited. Column **Grid Settings** can be added or removed or expanded and rearranged.

Click **Grid Settings**, and use the arrows next to the column **Name** to expand column options. A checkbox next to a name adds the selection to the grid.

Web Access

Select the **Web Access** tab to monitor status of AppFlow sessions that have **Web Access**. Application entries can be displayed as either limited or unlimited. Column **Grid Settings** can be added or removed, or expanded and rearranged.

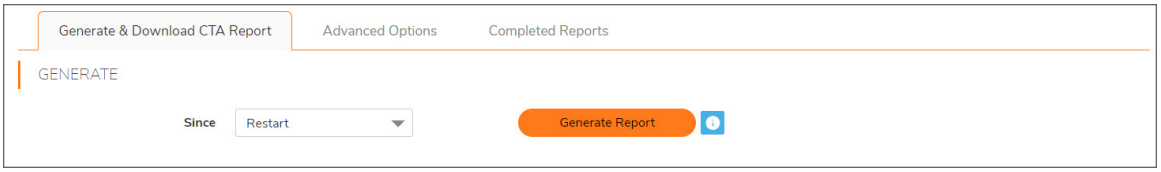
Click **Grid Settings**, and use the arrows next to the column **Name** to expand column options. A checkbox next to a name adds the selection to the grid.

4

CTA Report

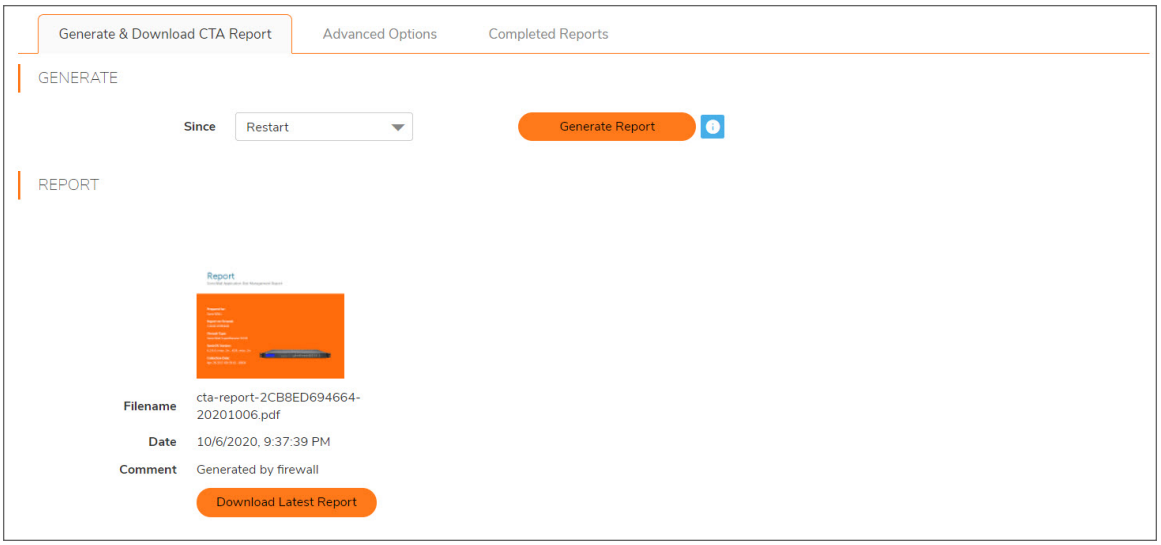
Use the Capture Threat Assessment (CTA) Report to generate a SonicFlow Report (SFR) that you can download and post to the Capture Threat Assessment service.

Generate & Download CTA Report



To generate and post the SonicFlow Report (SFR):

1. Navigate to the Capture Threat Assessment screen on the **MONITOR | AppFlow > CTA Report** page.
2. On the **Generate & Download CTA Report** tab, click **Generate Report**.
3. After the report is generated, you have the option to download the report or generate a new one.



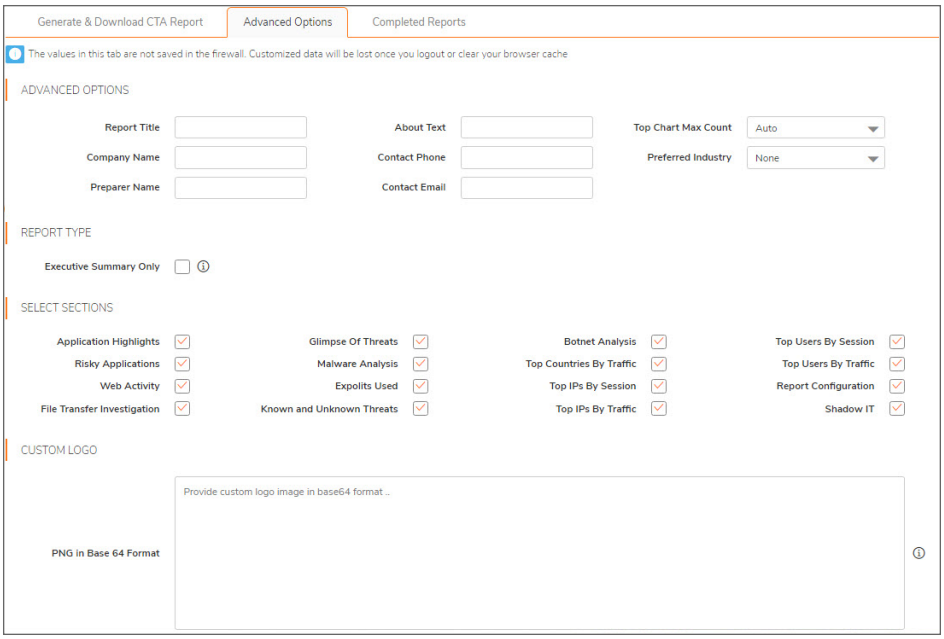
4. Click **Download Report** to download the report.

Advanced Options

The values on the **Advance Options** tab are not saved to the firewall. Customized data is lost after you log out or clear your browser cache.

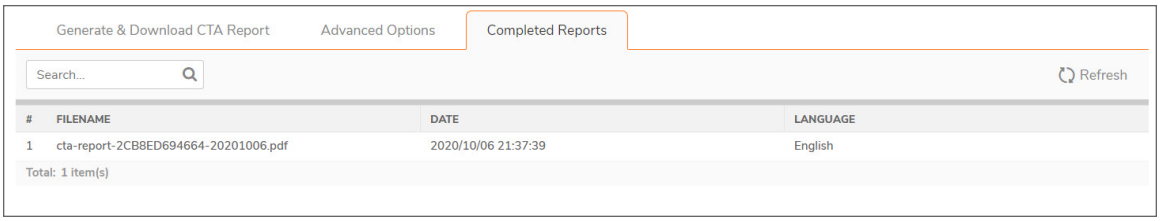
To configure Advanced CTA Report options:

1. Navigate to the **MONITOR | AppFlow > CTA Report** page.
2. Click the **Advanced Options** tab.



3. Customize data for your CTA Reports using Advanced Options, Report Types, Desired Sections to appear, or include a customized Report logo.
4. After completing customized data entries, return to **Generate & Download CTA Report** and click **Generate Report**. The customized Report appears in the **Completed Reports** tab.

Completed Reports



Generated reports appear in the table and are available for download, viewing, and deleting.

5

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.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

SonicOS Monitor AppflowAdministration Guide
Updated - May 2024
Software Version - 7.0
232-005326-00 Rev A

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