



Contents

AppFlow Report	3
Applications	4
Users	5
IP Addresses	6
Viruses	6
Intrusions	7
Spyware	7
Locations	8
Botnets	8
Web Categories	9
AppFlow Monitor	10
Applications	11
Users	12
Web Activity	12
Initiator IPs	13
Responder IPs	13
Threats	14
VoIP	14
VPN	15
Devices	15
Contents	16
Policies	16
AppFlow Sessions	17
All	18
Threats	18
Web Access	18
CTA Report	20
Generate & Download CTA Report	20
Advanced Options	21
Completed Reports	22
SonicWall Support	23
About This Document	24

AppFlow Report

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

ψ	Q Search • IP	/4 & IPv6 🛛 🖝	View: Sind	e Restart	•			Limit: 50	•	 • 	IE	1	ď	62	¢
			SESSIONS		INIT	TIATOR BYTES	RES	PONDER BYTES							
#	APPLICATION NAME	COUNT 🌲	PERCENTA	GE	COUNT	PERCENTAGE	COUNT	PERCENTAGE							
1	ど General HTTPS MGMT	75.96K		69%	113.80 MB	629	6 502.95 MB	47%							
2	Ceneral HTTPS	20.68K	-	18%	61.84 MB	349	6 208.14 MB	19%							
3	Ceneral DNS	9.17K		8%	1.10 MB	09	6 2.11 MB	0%							
4	Service NTP	1.51K	1	196	156.68 KB	09	6 155.12 KB	0%							
5	Service Version 2 Multicast Listener Report (IPv6)	1.05K		0%	89.24 KB	09	6 0 B	0%							
6	General HTTP	347		096	4.68 MB	. 29	6 338.04 MB	32%							
7	Service RPC Services (IANA)	130		096	33.01 KB	09	6 0 B	0%							
8	General HTTP MGMT	129		096	134.90 KB	09	6 3.53 MB	0%							
9	Service Echo	8		096	480 B	09	6 0B	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:

🔍 Search... + 19-4 & 1

1

- 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.

APPFLOW REPORT STATU	s			×
Aggregate A	ppFlow Repor	rting 🗸 E		
	Apps Report	rting 🧹 E		
	Using Sto	rage 🔺 D	isabled	
NAME	LICENSED	STATUS	SIGNATURES	TO CONFIGURE
Gateway Anti-Virus		Policy	Downloaded	Rules and Policies > Settings
Intrusion Prevention		Policy	Downloaded	
Anti-Spyware		Policy	Downloaded	Rules and Policies > Settings
Content Filtering		Policy	N/A	
Bandwidth Management	N/A	Advanced	N/A	
Country Database		N/A	Downloaded	N/A
Botnet Blocking		Policy	Downloaded	

• 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

- 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

- 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

	Applications	Users	IP Add	resses	Virus	Intrusion	ns Spy	ware	Locations	Botnet	ts Web	Catego	ories			
¢	Q Search		• IPv4	& IPv6 🔻	View: Since	Restart	•				~ •	⊨	<u>(</u>)	Ľ	<u>ر</u> ک	⇔
	COUNTRY MANY				SESSIONS		BY	TES RECEIV	ED	В	YTES SENT					
*	COUNTRY NAME			COUNT 🖡	PERCENTAG		COUNT	PERCENT	TAGE	COUNT	PERCENTAGE					
1	? Private			1.61M	_	96%	2.54 GB	_	80%	3.37 GB	_	91%				
2	? Unknown			55.70K		3%	615.20 MB	-	19%	340.77 MB	•	8%				

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.

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

Web Categories

	Applications Users	IP Add	dresses	Virus	Intrusion	s	Spyware	Locations	Botnets	Web Categories						
¢	Q Search	* IPv4	4 & IPv6 🛛 🔻	View: Sinc	e Restart	•					•	≔	<u>(</u> 9)	Ľ	₹2	۵
	DATING NAME			SESSIONS												
	RATING NAME		COUNT 🌲	PERCENTA	GE											
1	Information Technology/Compute	er	15.54K	_	50%											
2	Business and Economy		15.24K	-	49%											
з	Web Communications		121		096											
4	Search Engines and Portals		90		0%											
5	Computer and Internet Security		8		096											
6	Online Personal Storage		5		0%											

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

- 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

AppFlow Monitor

2

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 + Add to Filter *	Q Search	IPv4 & IPv6 🔻	0	All Flows	Group By: Application	•	+	 • 	🛃 Export	🗘 Refresh	Scolumn Selection
----------------------------	----------	---------------	---	-----------	-----------------------	---	---	-----------------------	----------	-----------	-------------------

- +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.

APPFLOW MONITOR STA	TUS			×
AppFlow t	o Local Collec Max Flows in I	tor 🗸 Ena DB 7500		
App Rules		Disabled		Rules and Policies > App Rules
Country Database				
Geo-IP Blocking		Disabled		
Botnet Blocking		Disabled	Not Downloaded	
Note: To configure, go to A				

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

Applications

			s Policies
	IPv4 & IPv6 ▼ 0 60 Secs 0	Group By: Application 🛛 👻 🔹	• 🗘 🌣
🛛 🗊 APPLICATIONS SESSIONS 🌲 TOTAL PACKETS TOTAL BYTES AVERAGE RATE (KBPS) THREATS	SESSIONS 👵 TOTAL PACKETS	TOTAL BYTES AVERAGE RATE (KBPS) THREATS	
□ 1 🚰 General HTTPS MGMT ♀ Q 31 180.26K 176.03 KB 1.494 0	ф Q 31 180.26К	176.03 KB 1.494	0
2 🚰 General TCP 🜵 Q 4 720 720 B - 0	¢ Q 4 720	720 B -	0
□ 3 🖉 General DNS ♀ Q 1 1.55K 1.52 KB 0.224 0	ф Q 1 1.56К	1.52 KB 0.224	0

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

Applica	ations	Users	Web Activity	Initiator IP	s	Responder I	Ps Threats	VoIP	VPN Devices	Contents		Policies	s
\$ 8	+ • [Q Search	IPv4	& IPv6 💌	•	60 Secs	o	G	Group By: User Name	• • 🗸 •	ď	<u>6</u> 2	¢
#	USERS					SESSIONS 🖊	TOTAL PACKETS	TOTAL BYTES	AVERAGE RATE (KBPS)	THREATS			
1	admin			\$	Q	47	183.02K	178.73 KB	0.208	0			
2	unknown			¢	Q	5	1.72K	1.68 KB	0.121	0			

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

Aj	pplications	Users	Web Activity	Initiator IPs	Responder I	IPs Threats	VoIP	VPN Devices	Contents	Policie	25
\$	\$ + →	Q Search	IPv4	& IPv6 🔻 💿	60 Secs	o	G	roup By: IP Address	• 🗸 •	0 10	\$
#	INITIATO	RIPS			SESSIONS 🖊	TOTAL PACKETS	TOTAL BYTES	AVERAGE RATE (KBPS)	THREATS		
1				\$ Q	48	180.38K	176.15 KB	0.208	0		
2				φ Q	2	2.50K	2.44 KB	0.223	0		
3				\$ Q	2	360	360 B	0.070	0		

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

Appli	ications	Users	Web Activit	y Initia	ator IPs		Responder I	Ps	Threats	VolP	VP	N Devices	Content	5	Polic	cies
\$	+ • [२ Search		IPv4 & IPv6	•	•	60 Secs		o		Grou	p By: IP Address	• 🗸	• C	5 t	2 ☆
#	RESPONDE	RIPS					SESSIONS 🖊	τοτα	L PACKETS	TOTAL BYTES	1	VERAGE RATE (KBPS)	THREATS			
1					ψ	Q	55		205.04K	200.24	КВ	0.541		0		
2					÷	Q	4		720	72	в	0.070		0		
3					÷	Q	2		2.01K	1.96	кв	0.246		0		
4					ψ	Q	1		503	50	в	0.240		0		

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

Image: Search Image: Search Image: Optimized Search Image: Optimized Search Imag	• • 🗹 •	ල් 🗘 🛠	¥
🖉 # POLICIES SESSIONS 🖡 TOTAL PACKETS TOTAL BYTES AVERAGE RATE (KBPS)	THREATS		
□ 1 Default Access Rule_15 ♀ Q 54 201.96K 197.23 KB 0.356	i c		
2 Default Access Rule_4 & Q 2 360 360 B 0.070) C		

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.

AppFlow Sessions

3

() | 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.

APPFLOW MONITOR STATUS X					
AppFlow to Loc Max F	al Collector Flows in DB	Disabled			
NAME	LICENSED	STATUS	SIGNATURES	TO CONFIGURE	
Gateway Anti-Virus	Yes	Policy	Downloaded	Rules and Policies > Setting	s
Intrusion Prevention	Yes	Policy	Downloaded	Rules and Policies > Setting	s
Anti-Spyware	Yes	Policy	Downloaded	Rules and Policies > Setting	s
Content Filtering	Yes	Policy	N/A	Rules and Policies > Setting	s
Bandwidth Management	N/A	Advanced	N/A	Profile Objects -> Bandwidt	th
Country Database	Yes	N/A	Downloaded	N/A	
Botnet Blocking	Yes	Policy	Downloaded	Rules and Policies > Setting	s
Note: To configure, go to AppFlow Settings > Flow Reporting.					

• 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.

CTA Report

4

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

Generate & Download CTA Report	Advanced Options	Completed Reports
GENERATE		
Since Restart	•	Generate 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.

Generate & Downloa	d CTA Report Advanced Options Completed Reports				
GENERATE					
	Since Restart Generate Report				
REPORT					
	Report .				
	Normal State				
Filename	cta-report-2CB8ED694664- 20201006.pdf				
Date	10/6/2020, 9:37:39 PM				
Comment	Generated by firewall				
	Download Latest Report				

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.

Generate & Download CTA	Report Advanced Op	tions Compl	eted Repor	ts				
The values in this tab are not sa	ived in the firewall. Customized d	ata will be lost once y	ou logout or	clear your browser cache				
ADVANCED OPTIONS								
Report Title		AI	bout Text		Top Chart Max Count	Auto	•	
Company Name		Conta	ct Phone		Preferred Industry	None	-	
Preparer Name		Cont	act Email					
REPORT TYPE								
Executive Summary Only								
SELECT SECTIONS								
Application Highlights		Glimpse Of Threats	\checkmark	Botnet An	alysis 🗹	Top Users By S	Session 🗹	
Risky Applications		Malware Analysis	\checkmark	Top Countries By 1	raffic 🗹	Top Users By	Traffic 🗹	
Web Activity		Expolits Used	\checkmark	Top IPs By Se	ssion 🗹	Report Configu	uration 🗹	
File Transfer Investigation	Known and	d Unknown Threats		Top IPs By 1	'raffic 🗹	Sha	dow IT 🔽	
CUSTOM LOGO								
	Provide custom logo image i	n base64 format						
PNG in Base 64 Format								(i)

- 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

Generate & Download CTA Report Advanced Optic	Completed Reports	
Search Q		🗘 Refresh
# FILENAME	DATE	LANGUAGE
1 cta-report-2CB8ED694664-20201006.pdf	2020/10/06 21:37:39	English
Total: 1 item(s)		

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

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

Copyright © 2024 SonicWall Inc. All rights reserved.

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