SonicWall® Analytics REPORTS

Administration

For a Syslog-Based Solution

SONICWALL®

Contents

1

REPORTS Overview

This document introduces the **REPORTS** view for the Syslog-based Analytics solution. This solution can be used as a stand-alone solution or it can be used with a SonicWall firewall management system, such as CSC-MA or GMS (Global Management System). You can evaluate the data and gain insight into your network, user access, connectivity, application use, threat profiles and other firewall-related data.

ⓘ **NOTE:** Syslog-based Analytics requires its own license agreement. The license has to be associated with a firewall in your system.

Topics:

- Description
- Default Page
- Navigation
- Device vs. Global Reports

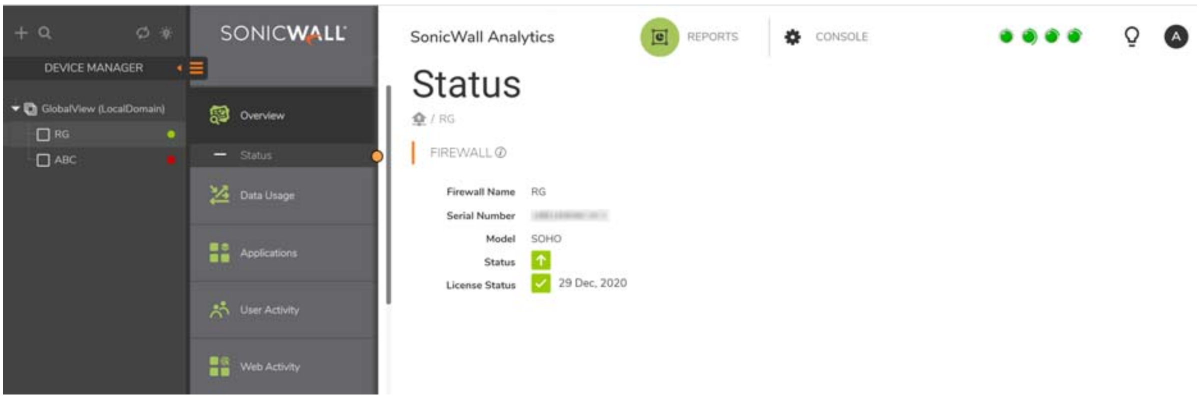
Description

The Syslog-based REPORTS option is a reporting tool that provides you with real-time insight into the health, performance and security of your networks. Using a variety of customizable reports with drill-down capabilities, the activity on your firewall is organized to show real-time and historical insights into network health, performance, and security. Benefits include:

- Comprehensive graphical reports enable visibility and analysis of threats and activities.
- Syslog reporting streamline data summarization.
- Universal scheduled reports speed in-depth reporting.
- At-a-glance reporting facilitates quick analysis.
- Compliance reporting makes report generation easy.
- Multi-threat reporting provides instant information on threats and attacks.
- User-based reporting tracks activity across the entire network.
- New attack intelligence enables granular reporting on.

Default Page

When you first log into Syslog-based Analytics, the default page displayed is the **Overview > Status** page, with the status of the first device in the list being shown.



Status

/ RG

FIREWALL

Firewall Name RG

Serial Number [redacted]

Model SOHO

Status ↑

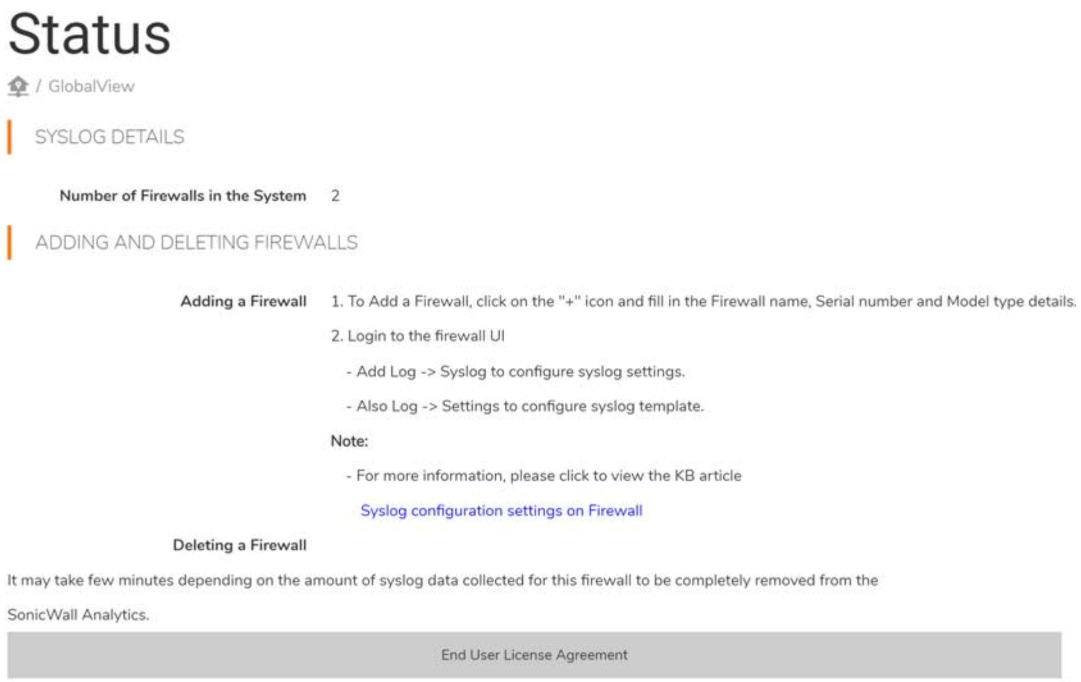
License Status ✓ 29 Dec, 2020

The Status pages shows the firewall name, serial number, model, operational status and license status.

NOTE: The **License Status** displays three different states: green indicates that the Analytics license is active and you have access to reports. When you first buy a firewall, you have an automatic grace period of a few day where you can access the Syslog-based Analytics reports. Orange indicates that your license (or the grace period) is about to expire, and red indicates that the license has expired. Go to https://mysonicwall.com/muir/login/step2 to renew your license.

IMPORTANT: If your license expires, your data is still visible until it ages out. The age-out time is based on the data deletion schedule you defined at **CONSOLE > Summarizer > Data Deletion Schedule**.

If you select the GlobalView on the Device Manager, the Status pages changes to reflect the new view. You can see the number of firewalls in the system and information on how to add and delete firewalls into the Analytics reporting.



Status

/ GlobalView

SYSLOG DETAILS

Number of Firewalls in the System 2

ADDING AND DELETING FIREWALLS

Adding a Firewall

1. To Add a Firewall, click on the "+" icon and fill in the Firewall name, Serial number and Model type details.
2. Login to the firewall UI
   - Add Log -> Syslog to configure syslog settings.
   - Also Log -> Settings to configure syslog template.

Note:

- For more information, please click to view the KB article
  Syslog configuration settings on Firewall

Deleting a Firewall

It may take few minutes depending on the amount of syslog data collected for this firewall to be completely removed from the SonicWall Analytics.

End User License Agreement

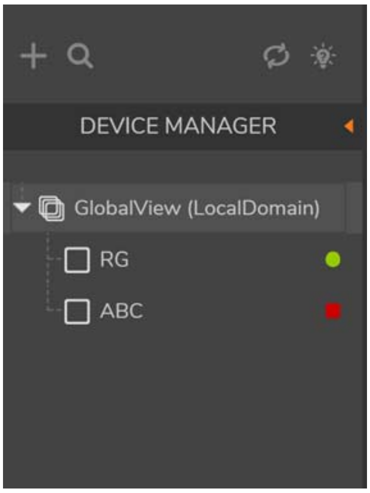
Navigation

Navigating the Syslog-based Analytics reports is quite easy. The interface has three main sections of information.

- Device Manager
- Command Menu
- Work Space

Device Manager

In the far left column, the **DEVICE MANAGER** , you can choose your view. Syslog-based reporting offers the option to see the **GlobalView** which is a compilation of the all the firewalls in your setup, or you can select an individual firewall to view. The following example shows the **GlobalView** selected, and the system is setup with two firewalls: one is up and one is down.



You can hide the **DEVICE MANAGER** by clicking on the orange **Collapse** option.

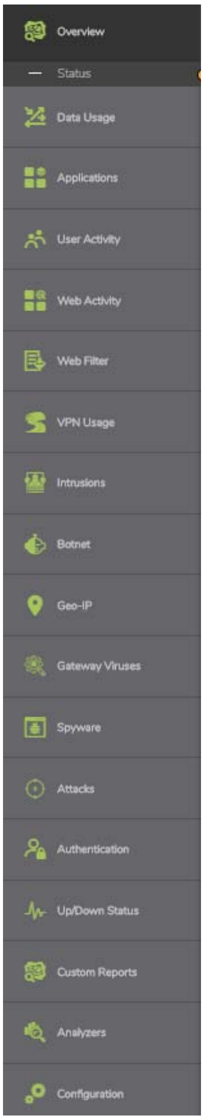
Use the icons above the **DEVICE MANAGER** title to facilitate your work in this space.

- Click on the **Add Unit (+)** icon to add a firewall.
- Click on the **Search** icon to look for a firewall.
- Click on the **Reload Device Manager** icon to refresh the Device Manager.
- Click on the **Help** icon to see the Firewall State Icon Legend.

Command Menu

The command menu is located directly under the SonicWall logo. You can manage your devices in the **REPORTS** view using these commands. The commands are grouped under similar functions. Click on the command to expand it and see the options. For example, expand Data Usage to see the five different reports listed under it.

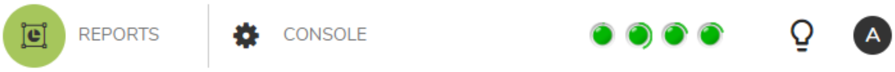
ⓘ **NOTE:** If you select a different option, or view, from the top of the work area, different menu items are shown in this space.



Work Space

The work space is where all the data is displayed. On the **REPORTS** view this is where you see reports and set parameters. GMS 9.2 and CSC-MA 1.7 group similar tasks under the views identified by the icons across the top navigation of the work space.

Other command options and information are available by selecting the icons across the top of the section:



Click on the **CONSOLE** icon to access other commands related to reporting. You can configure and view logs as well as customize and schedule reports. Refer to the *Analytics CONSOLE Administration Guide* for details.

The status lights are a quick indicator of system health, and the color varies based accordingly. When you click on them, they show more details on:

- CPU/Processor
- Memory/RAM
- Storage/Disk
- Estimated Capaticy

Device vs. Global Reports

Several different Syslog-based reports have been predefined for your use. All reports have a device or unit view; a subset of those also have a global view. The reports offer a graphical representation of the data and/or a table showing the details. The following table shows what is data is available for each view.

Syslog-Based Reports **Unit Level**	**Syslog-Based Reports** **Global Level**
Overview • Status	**Overview** • Status
Data Usage • Timeline • Initiators • Responders • Services • Details	**Data Usage** • Summary
Applications • Data Usage • Detected • Blocked • Categories • Initiators • Timeline	**Applications** • Summary
User Activity • Details	Not applicable
Web Activity • Categories • Sites • Initiators • Timeline • Details	**Web Activity** • Summary • Top Categories • Category Details
Web Filter • Categories • Sites • Initiators • Timeline • Details	**Web Filter** • Summary • Top Categories • Category Details

Syslog-Based Reports **Unit Level**	**Syslog-Based Reports** **Global Level**
VPN Usage • Policies • Initiators • Services • Timeline	**VPN Usage** • Summary
Not applicable	**Threats** • Summary
Intrusions • Detected • Blocked • Targets • Initiators • Timeline • Details • Alerts	**Intrusions** • Top Detected • Detected Details
Botnet • Initiators • Responders • Attacks • Timeline	Not applicable
Geo-IP • Responder Countries • Initiator Countries	Not applicable
Gateway Viruses • Blocked • Targets • Initiators • Timeline • Details • Alerts	**Gateway Viruses** • Summary • Top Blocked • Blocked Details
Spyware • Detected • Blocked • Targets • Initiators • Timeline • Details • Alerts	Not applicable
Attacks • Attempts • Targets • Initiators • Timeline	Not applicable
Authentication • User Login • Admin Login • Failed Login	Not applicable

Syslog-Based Reports **Unit Level**	**Syslog-Based Reports** **Global Level**
Up/Down Status • Timeline	Not applicable
Custom Reports • Manage Reports	Not applicable
Analyzers • Log Analyzer	Not applicable
Configuration • Settings • Syslog Filter	**Configuration** • Settings

Related Documents

The following documents provide additional information about Analytics or related firewall management applications:

- *Analytics HOME Administration*
- *ANALYTICS Administration*
- *Analytics NOTIFICATIONS Administration*
- *Analytics CONSOLE Administration Guide*

2

Reporting Details

On-Premises Analytics 2.5 offers Syslog-based reporting to protect an organization’s operations and network security. Syslog reports drill down on the firewall data to evaluate the risk that certain types of applications and websites can pose on a network security system.

ⓘ | **NOTE:** Syslog-based reporting and IPFIX-based reporting cannot be offered simultaneously.

Topics:

- Verifying Syslog Status
- Data Usage
- Applications
- User Activity
- Web Activity
- Web Filter
- VPN Usage
- Threats
- Intrusions
- Botnet
- Geo-IP
- Gateway Viruses
- Spyware
- Attacks
- Authentication
- Up/Down Status
- Custom Reports
- Analyzers
- Configuration
- Scheduling Reports

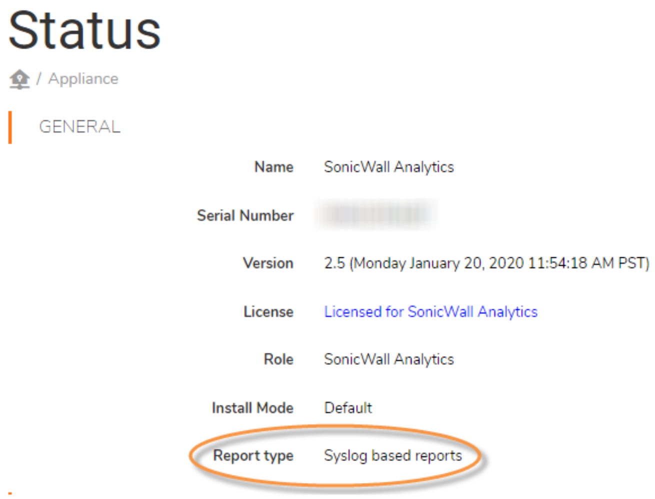
Verifying Syslog Status

To verify the Syslog reports option:

1 On your Analytics system, navigate to **CONSOLE | Appliance > Appliance**.

The left-hand menu automatically changes taking you to the appliance **Status** page.

2 Under the **GENERAL** section, make sure you have **Syslog-based reports** next to **Report type**.



Status

/ Appliance

GENERAL

Name SonicWall Analytics

Serial Number

Version 2.5 (Monday January 20, 2020 11:54:18 AM PST)

License Licensed for SonicWall Analytics

Role SonicWall Analytics

Install Mode Default

Report type Syslog based reports

3 Select **Analytics > Console** to navigate back to the **REPORTS** view.

Data Usage

The **Data Usage** group of reports collects the data related information in one place. These reports display a graph of the data by default. Some are presented in a bar chart; others in a pie chart. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

To filter the data to meet specific criteria:

1 Click on the **Filter** icon.

2 Enter the Boolean criteria and filter values.

3 Click the **Reload** icon to refresh the data.

4 To remove the filter, click on the **x** in the filter bar and reload the data.

When in the device or unit level view, you can access the following reports:

Timeline	Shows how many connections are being made each hour and how much data is being transferred. By default this data shown in a bar graph followed by a table that also includes the cost. You can adjust the timeline on the graph or you can hide graph and just see the table. Totals are shown at the bottom of the page.
Initiators	Shows the information on those initiating the data transactions. It includes their IP addresses, their host names, MAC address, user name, and it identifies how many connections the initiator has and how much data is transferred (gigabytes).
Responders	Lists the top responders, their IP addresses, their responder host names, and MAC address. It also show how many connections the responder had and the number of gigabytes transferred.
Services	Shows the connections listed by service protocol. It also shows the number of connections and the number of gigabytes transferred.
Details	Provides a a view to multiple reports from a single command. Each of the above reports can be viewed by selecting the appropriate tab above the graph. Additional reports show geographical data like **Initiator Countries** and **Responder Countries**. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details.

When in **GlobalView**, a summary of the data usage is provided for the active devices in the system.

Applications

The **Application** group of reports collects the application related information in one place. These reports display a graph of the data by default.The time period of the chart can be customized, or the chart can be hidden from view.

A filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Data Usage	**A**llows you to see the connections, listed by application and threat level for the time period selected.
Detected	Allows you to see the events detected, listed by application and threat level for the time period selected.
Blocked:	Shows the blocked events, listed by application and threat level for the time period selected.
Categories:	Lists the application categories attempting access for the time period selected.
Initiators:	Shows the Initiator IP address, Initiator host, user, events and transferred data events for the time period selected.
Timeline:	Shows the timeline, time, events and transferred data over the time period selected.

When in GlobalView, a summary of the application-related data is provided for the active devices in the system.

User Activity

The **User Activity > Details** report allows you to see data for a specified user. When you first select the report, the filter is open and asks that you filter against a specific user before using other filters to drill down. Once you identify the user, the system provides several reports based on the data available. You can filter the data further, or you can view the different views of the data by clicking on the tabs.

ⓘ **NOTE:** You may need to scroll to the right and left to see all the report tabs.

As with other reports, you can customize the time period or hide the graph.

When in **GlobalView**, the **User Activity** reports are not available.

Web Activity

The **Web Activity** group of reports collects the web activity information in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Categories	Shows the browse time and hits for each category of web activity. The web activity category may be something like email or search engines and portals. It shows data for the time period selected.
Sites	Shows information about the sites visited, such as IP address, site name, and category. The table also includes the number of hits and browse time for each site, as well as how much data was transferred.
Initiators	Shows the Initiator IP address, initiator host, MAC address, and user name. It also shows the browse time, number of hits and the data transferred. The data covers the time period selected.
Timeline	Shows the time of access and browse time as well as the number of hits and how much data was transferred. Totals are shown at the bottom of the page.
Details	Provides a a view to multiple reports from a single command. Each of the above reports can be viewed by selecting the appropriate tab above the graph. Additional reports show geographical data like **Initiator Countries** and **Responder Countries**. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details.

When in **GlobalView**, a three different reports are provided for **Web Activity**:

Summary	Shows the hits and amount of data transferred, listed by appliance. The data covers the time period selected, and totals are shown at the bottom.

Top Categories	Shows the top web categories being browsed, browse time, hits and amount of data transferred. The data covers the time period selected, and totals are shown at the bottom.
Category Details	Provides a a view to multiple reports from a single command. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details. The data covers the time period selected, and totals are shown at the bottom.

Web Filter

The **Web Filter** group of reports collects the web filtering information in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Categories	Shows the category type and number of attempts for each. It shows data for the time period selected.
Sites	Shows information about the sites visited, such as IP address, site name, category, and the number of attempts. The data covers the time period selected.
Initiators	Shows the Initiator IP address, initiator host, user name and number of attempts. The data covers the time period selected.
Timeline	Shows the time of access and the number of attempts. Totals are shown at the bottom of the page.
Details	Provides a a view to multiple reports from a single command. Each of the above reports can be viewed by selecting the appropriate tab above the graph. Additional reports show geographical data like **Initiator Countries** and **Responder Countries**. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details.

When in **GlobalView**, a three different reports are provided for **Web Activity**:

Summary	Shows the number of attempts, listed by appliance. The data covers the time period selected, and totals are shown at the bottom.
Top Categories	Shows the top web categories being browsed and the number of hits. The data covers the time period selected, and totals are shown at the bottom.
Category Details	Provides a a view to multiple reports from a single command. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details. The data covers the time period selected, and totals are shown at the bottom.

VPN Usage

The **VPN Usage** group of reports collects the VPN usage information in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Policies	Shows the VPN policy, number of connections managed by that policy and the amount of data transfered. It shows data for the time period selected.
Initiators	Shows the Initiator IP address, initiator host, and user name. It also shows the number of connections and the data transferred. The data covers the time period selected.
Services	Shows the connections listed by service protocol. It also shows the number of connections and the number of gigabytes transferred.
Timeline	Shows the time of access, the number of connections and how much data was transferred. Totals are shown at the bottom of the page.

When in **GlobalView**, a summary of the VPN usage data is provided for the active appliances in the system. It includes the number of connections and the amount of data transferred. The totals are summarized at the bottom of the table.

Threats

While the device view does not have a section for **Threats** reports, the **GlobalView** does have a **Threats > Summary** report. It summarizes the number of threat attempts that were made on each appliance. You can change the time period and hide the graph. You can also filter the data being displayed to see a more specific dataset.

Intrusions

The **Intrusions** group of reports collects the intrusion data in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Detected	Shows the intrusions detected, the priority threat and the events. It shows data for the time period selected.
Blocked	Shows the intrusion blocked, the priority threat and the events. It shows data for the time period selected.
Targets	Shows the target IP address, target host, and number of events. The data covers the time period selected.

Initiators	Shows the initiator IP address, initiator host, user name and number of events. The data covers the time period selected.
Timeline	Shows the time of access and the number of events. Totals are shown at the bottom of the page.
Details	Provides a a view to multiple reports from a single command. The reports can be viewed by selecting the appropriate tab above the graph. Reports showing geographical data like **Initiator Countries** and **Responder Countries** are also included. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details.
Alerts	The LOG ANALYZER alerts are shown in this table.

When in **GlobalView**, a two different reports are provided for **Intrusions**:

Top Detected	Shows the top intrusions detected. It includes the intrusion name and the events. The data covers the time period selected, and totals are shown at the bottom.
Detected Details	Provides a a view to multiple reports from a single command. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details. The data covers the time period selected, and totals are shown at the bottom.

Botnet

The **Botnet** group of reports collects the botnet information in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Initiators	Shows the initiator IP address, initiator country, initiator host, and events. The data covers the time period selected.
Responders	Shows the target IP address, responder country, target host, and events. The data covers the time period selected.
Attacks	Shows information on the botnet attacks. It includes the botnet IP address, the threat, the severity level, country, the active state, the URL and the events. The data covers the time period selected.
Timeline	Shows the time line for the botnet events. Totals are shown at the bottom of the page.

When in **GlobalView**, **Botnet** reports are not available.

Geo-IP

The **Botnet** group of reports collects the botnet information in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Initiator Countries	Shows the Geo-IP events, by initiator, that were blocked and what country they were from. The data covers the time period selected.
Responder Countries	Shows the Geo-IP events, by responder, that were blocked and what country they were from. The data covers the time period selected.

When in **GlobalView**, **Geo-IP** reports are not available.

Gateway Viruses

The **Gateway Viruses** group of reports collects the gateway virus data in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Blocked	Shows the gateway viruses that were blocked, the action taken and the events. It shows data for the time period selected.
Targets	Shows the target IP address, target host, and number of events. The data covers the time period selected.
Initiators	Shows the initiator IP address, initiator host, user name and number of events. The data covers the time period selected.
Timeline	Shows the time of access and the number of events. Totals are shown at the bottom of the page.
Details	Provides a a view to multiple reports from a single command. The reports can be viewed by selecting the appropriate tab above the graph. Reports showing geographical data like **Initiator Countries** and **Target Countries** are also included. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details.
Alerts	The LOG ANALYZER alerts are shown in this table.

When in **GlobalView**, a three different reports are provided for **Gateway Viruses**:

Summary	Shows the number of blocked events for each appliance. The data covers the time period selected, and totals are shown at the bottom.
Top Blocked	Shows the top viruses blocked. It includes the virus name, the actions and the events. The data covers the time period selected, and totals are shown at the bottom.
Blocked Details	Provides a a view to multiple reports from a single command. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details. The data covers the time period selected, and totals are shown at the bottom.

Spyware

The **Spyware** group of reports collects the spyware data in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Detected	Shows the spyware that was detected, the priority and the events. It shows data for the time period selected.
Blocked	Shows the spyware that was blocked, the priority and the events. It shows data for the time period selected.
Targets	Shows the target IP address, target host, and number of events. The data covers the time period selected.
Initiators	Shows the initiator IP address, initiator host, user name and number of events. The data covers the time period selected.
Timeline	Shows the time of access and the number of events. Totals are shown at the bottom of the page.
Details	Provides a a view to multiple reports from a single command. The reports can be viewed by selecting the appropriate tab above the graph. Reports showing geographical data like **Initiator Countries** and **Target Countries** are also included. By clicking on the Search icon in the table, you are taken to the **Log Analyzer** where you can drill down for more details.
Alerts	The LOG ANALYZER alerts are shown in this table.

When in **GlobalView**, **Spyware** reports are not available.

Attacks

The **Attacks** group of reports collects the attack data in one place. These reports display a graph of the data by default. The time period of the chart can be customized, or the chart can be hidden from view.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

Attempts	Shows the attacks that were detected and the events. It shows data for the time period selected.
Targets	Shows the target IP address, target host, target MAC address and number of events. The data covers the time period selected.
Initiators	Shows the initiator IP address, initiator host, initiator MAC address, user name and number of events. The data covers the time period selected.
Timeline	Shows the time of access and the number of events. Totals are shown at the bottom of the page.

When in **GlobalView**, **Spyware** reports are not available.

Authentication

The **Authentication** group of reports collects the data about user and administrator authentication in one place. These reports display a graph of the data by default. The time period of the table can be customized.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them.

When in the device or unit level view, you can access the following reports:

User Login	Shows a log of the user logins. Data includes time, initiator IP address, user name, initiator host name, initiator MAC address, duration of the session, service used and messages about the session.
Admin Login	Shows a log of the admin logins. Data includes time, initiator IP address, user name, initiator host name, initiator MAC address, duration of the session, service used and messages about the session.
Failed Login	Shows the failed logins to your system. Data includes time, initiator IP address, user name, initiator host name, initiator MAC address, duration of the session, service used and messages about the session.

When in **GlobalView**, **Authentication** reports are not available.

Up/Down Status

The **Up/Down Status > Timeline** report shows you the time, up time, down time, up time percentage, displayed over time. A graph of the data is displayed by default, but can be hidden. The time period of the table can be customized.

When in **GlobalView**, **Up/Down Status** reports are not available.

Custom Reports

Manage your custom reports in this area. You can select and edit the reports or you can delete them.

For information on how to define custom reports, refer to *Analytics CONSOLE Administration Guide* for more information.

Analyzers

The **Analyzers > Log Analyzer** report provides a detailed, event-by-event listing of all activity. By clicking on the Search icon in the Log Analyzer table you can drill down those specific fields. The table provides the time, initiator IP address, initiator host address, user name when known, SRC port information, SRC interface, responder IP address, destination port, destination interface and responder host URL.

A sophisticated filtering tool is provided so you can limit or redefine what data is displayed in the reports. The filter uses Boolean operators and user-defined filter values. It also provides some built-on filter options if you want to use them. Be sure to reload the data after defining or deleting a filter.

Configuration

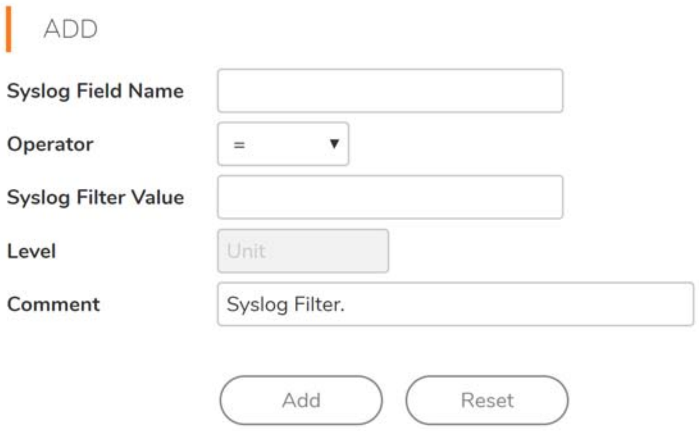
When in either **GlobalView** or the device view, you can set the **SUMMARIZER SETTINGS** for the data usage reports.

1. Navigate to **Configuration > Settings**.
2. Select the **Type of Currency** from the drop-down menu.
3. Enter the **Cost per Megabyte Data Use** in the field provided.
4. Click **Update**.

When in the device view you can also set up an **SYSLOG EXCLUSION FILTER**. The Syslog Exclusion Filter applies only to the syslogs uploaded to the reporting database. All syslogs continue to be stored in the file system without any filtering. Exclusion Filter settings are picked up by the Summarizer every 15 minutes.

To add a SYSLOG EXCLUSION FILTER:

1. Navigate to **Configuration > Syslog Filter**.
2. Click the **Add** button.



ADD

Syslog Field Name	
Operator	=
Syslog Filter Value	
Level	Unit
Comment	Syslog Filter.

3. Type in the **Syslog Field Name**.
4. Select the **Operator** from the drop-down list.
5. Type the **Syslog Filter Value** in the field provided.
6. Add any notes to the **Comment** field.
7. Click **Add**.

To delete a SYSLOG EXCLUSION FILTER:

1. Navigate to **Configuration > Syslog Filter**.
2. Select a filter from the list.
3. Click **Delete**.

Scheduling Reports

You can define and schedule custom reports. Navigate to **CONSOLE > Reports > Scheduled Reports**. Refer to the *Analytics CONSOLE Administration Guide* for details.

3

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.

Analytics **REPORTS** Administration for a Syslog Solution
Updated -January 2020
232-005212-00 Rev A

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

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

End User Product Agreement

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

Open Source Code

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

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