

SonicWall[®] Analytics HOME

Administration

SONICWALL[®]

Contents

About Analytics	4
Understanding Analytics	4
Using On-Premises Analytics	5
Using Analytics with CSC-MA	5
Navigation	5
Device Manager	6
Command Menu	6
Work Space	6
Notification Center	7
Monitoring Firewall Acquisition	8
Related Documents	8
Device Manager	9
Device Manager Views	9
Using the Device Manager	10
Appliance Status	12
Overview	13
Status	13
Acquisition History	14
Firewall	14
Network	14
Management	15
Reporting	15
Subscription	16
Firewall Information	16
Fetch Information	16
Synchronize with MySonicWall.com	16
End User License Agreement	17
Dashboard	17
SYSTEM HEALTH/TOP ATTACKS	18
TRAFFIC MAP	19
Dashboard Side Bar	19
Live Monitor	19
Devices	21
Device List	21
Devices	22
Summary	24
Navigating the Summary Reports	25
Customizing Summary Reports	25
Managing the Report Panels	25
Applications	26
Users	27

Viruses	27
Intrusions	28
Spyware	29
Botnet	29
Web Categories	29
Sources	30
Destinations	31
Source Locations	31
Destination Locations	32
BW Queues	32
Blocked	32
Threats	32
Capture ATP	33
Status	33
SonicWall Support	35
About This Document	36

About Analytics

This chapter introduces SonicWall® Analytics. Analytics is designed to evaluate data collected by the firewall ecosystem, make policy decisions and take defensive actions using application- and user-based analytics.

i **NOTE:** The Syslog-based implementation of On-Premises Analytics does not include a **HOME** view. Key Syslog-based information is provided in the **REPORTS** view. Refer to *Analytics REPORTS Administration* for more information.

Topics:

- [Understanding Analytics](#)
- [Navigation](#)
- [Notification Center](#)
- [Monitoring Firewall Acquisition](#)
- [Related Documents](#)

Understanding Analytics

SonicWall Analytics extends security event analysis and reporting by providing real-time visualization, monitoring and alerts based on the correlated security data. You can perform flexible drill-down and gain insight into your network, user access, connectivity, application use, threat profiles and other firewall-related data. Analytics provides the following key features:

- Data collection that includes normalizing, correlating, and contextualizing the data to the environment
- Streaming analytics in real time
- Analytics including activity trends and connections across the entire network
- Real-time, dynamic visualization of the security data from a single point
- Real-time detection and remediation

SonicWall Analytics is flexible and designed to integrate into other SonicWall solutions:

- On-Premises Analytics is designed for customers requiring long term storage of firewall logs and supports designated SonicWall firewalls.
- Analytics can also be integrated with Capture Security Center-Management, Reporting, and Analytics (CSC-MA).

Analytics offers either Syslog- or IPFIX-based analytics and reporting. You can choose one or the other based on your data needs. Using both styles in a dual mode is not offered at this time.

Using On-Premises Analytics

The IPFIX-based Analytics can be used as a standalone on-premises solution for collecting and storing flows data from firewalls not being managed collectively. It can be deployed as a virtual machine using OVA on VMware ESXi. Refer to the On-Premises Analytics ESXi Deployment Guide, which can be found at the [Technical Documentation portal](#).

NOTE: In this kind of deployment, you do not have firewall management capabilities.

Using Analytics with CSC-MA

SonicWall Analytics can also be used in conjunction with CSC-MA. This allows users to manage firewalls from CSC-MA and also view reporting and analytics data in CSC-MA from On-Premises Analytics while storing data locally.

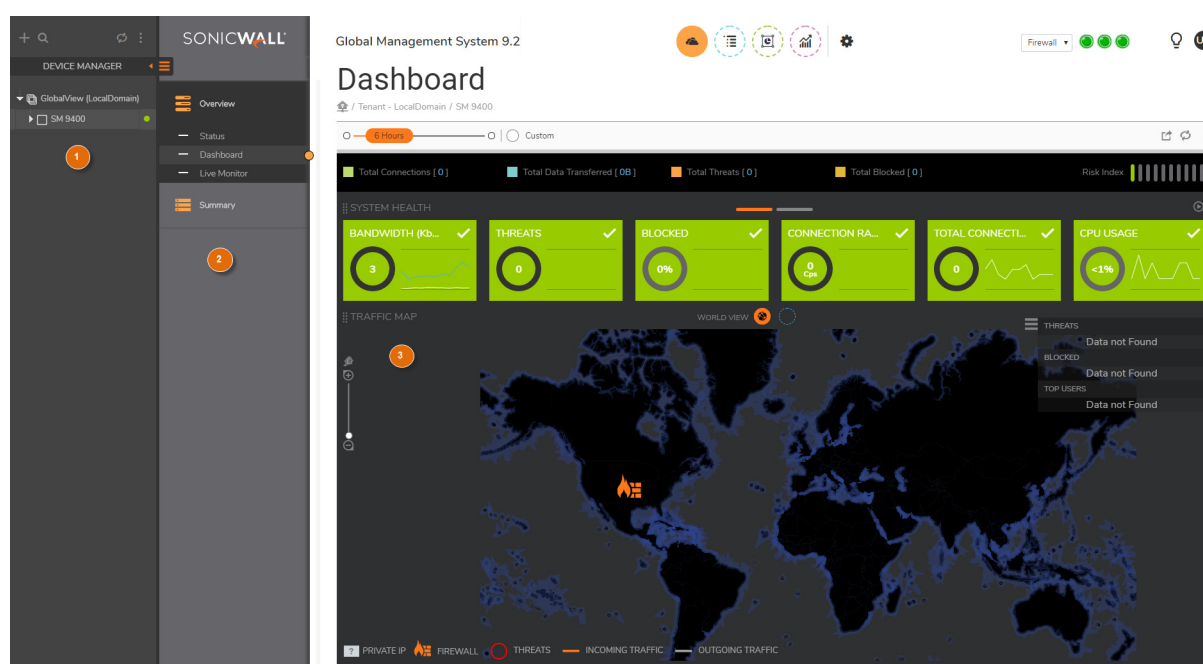
When you click on the firewall whose data is stored in Analytics, CSC-MA fetches the data from the On-Premises Analytics and shows it in CSC-MA. Data is encrypted and compressed so that no data integrity issues are experienced.

Navigation

The interface for Analytics varies because of the different configurations and types of reporting that can be selected. The images provided do not match every implementation, but should be viewed as an example that you can use as a guide while moving through the interface. Major differences are noted when needed to avoid confusion.

When you first open the **HOME** view, the interface shows three work areas:

- 1 Device Manager
- 2 Command menu
- 3 Work space



Device Manager

In the **DEVICE MANAGER**, you can group the devices in your security infrastructure using the pre-defined views. Under each view you see a summary of all of the devices that are being managed in your security infrastructure. The appliances are listed in alphabetic order. You can change the views, and additional views include:

- GlobalView
- FirmwareView
- ModelView.

In FirmwareView and ModelView, the devices are grouped by firmware version and model number, respectively. Refer to [Device Manager](#) for more information.

Command Menu

The command menu is located directly under the SonicWall logo. You can manage your devices using these commands. The commands are grouped under similar functions. Click on the command to expand it and see the options. For example, **Status**, **Dashboard**, and **Live Monitor** are grouped under **Overview** for IPFIX-based reporting. If you select a different view from the top of the work area, different menu items are shown.

Work Space

The work space is where all the data is displayed. This is where you monitor status, see reports, set schedules, drill down for data and so forth. Similar tasks are grouped under the views identified by the icons across the top navigation of the work space. The options may vary according to your configuration. The following figures shows two sample implementations, along with a description of the views.

Top Navigation for Syslog-Based, On-Premises Analytics



Top Navigation for Analytics in CSC-MA



Icon	Description
HOME	The default view when you login with most implementations. Navigate here to view the general data such as status, Dashboard, and summary reports. NOTE: The Syslog-based, On-Premises Analytics is missing the HOME view.
MANAGE	When Analytics is licensed with a firewall management system this view takes you to the commands for managing your firewalls.
REPORTS	Various reports, including live reports, when available, are shown and scheduled in this view.
ANALYTICS	Available for the IPFIX-based Analytics. Navigate here to see details and perform a deep dive on the information.

Icon	Description
NOTIFICATIONS	Shows the status of your network system, allows you to set rules and configure settings, and shows the history of the rules. NOTE: This view is available with only with IPFIX-based Analytics.
CONSOLE	Provides access to the CONSOLE (also labeled the Application Configuration Panel on the interface) where you can view logs, manage your appliance and perform other tasks.

At the upper right corner of the work space, additional icons provide information and facilitate your work.



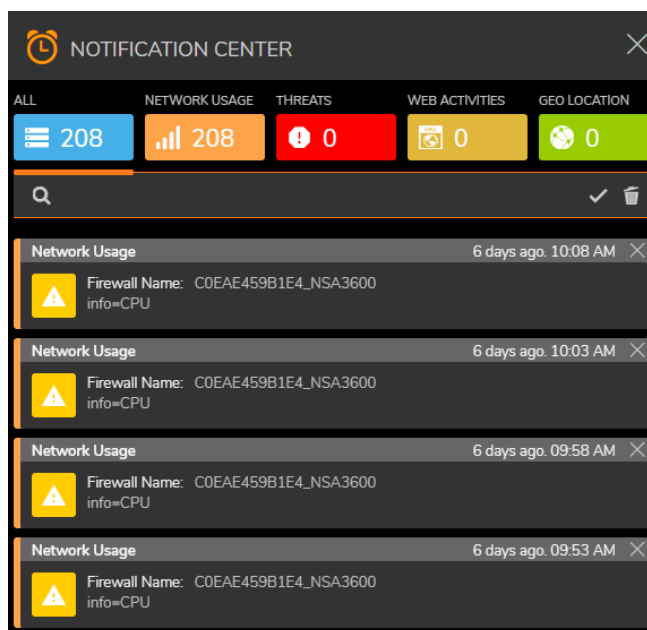
Icons	Description
Appliance text box	Indicates the type of device being monitored.
System Status icons	Provides system status. Click the individual icons for more detail. <ul style="list-style-type: none"> • CPU/Processor • Memory/RAM • Storage/Disk • Estimated Capacity (shown for On-Premises Analytics implementations)
Alerts and Notifications icon	Opens the Alerts and Notifications Center. (Refer to Notification Center for more information.) NOTE: This is only available with IPFIX-based Analytics operating in a cloud environment.
Online Help	Accesses the online help and the Analytics API.
User ID	Indicates the user and the version of the product, and allows you to log out of the application.

Notification Center

NOTE: The Notification Center is only available with IPFIX-based Analytics operating in a cloud environment.

The Notification Center provides an overview of the status and activities being monitored and recorded by Analytics. It displays all alerts, network usage, threats, web activities, and geo (geological) locations. Each option shows how many unread alerts appear in that particular category.

Tile	Description
ALL	Shows the all alerts for all the categories.
NETWORK USAGE	Shows the alerts generated specifically by network usage.
THREATS	Shows the alerts generated by threats such as botnet, virus, intrusion, spyware, and so forth.
WEB ACTIVITIES	Shows alerts generated by websites and web categories.



In the search bar, you can search by firewall name, alert name, message or details.

To mark a single alert as read, click on the alert to acknowledge it. Click the white checkmark to mark all alerts in that view as having been read.

To delete a single alert, click on the **X** on each alert. Click the trash icon at the top right to delete all the alerts in the view.

Monitoring Firewall Acquisition

When acquiring a firewall, regardless of the implementation, the system reports the steps so you can monitor the progress. It monitors both Zero Touch Deployments or systems set up manually. Navigate to the **Overview > Status** page to monitor the acquisition. General steps may include:

- Unit Setup
- Unit Acquisition
- Reporting and Analytics Setup
- Finished

Related Documents

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

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

Device Manager

This chapter explains the functionality of the **DEVICE MANAGER**, a tool that lists your registered appliances in your security infrastructure using pre-defined views.

Topics:

- [Device Manager Views](#)
- [Using the Device Manager](#)
- [Appliance Status](#)

Device Manager Views

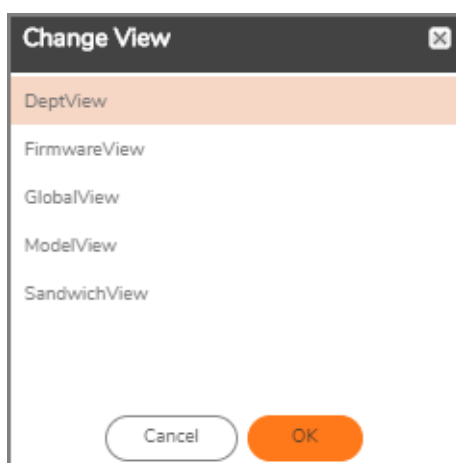
The devices are listed in alphabetical order in the **DEVICE MANAGER**, but you can view the appliances in groupings, or views, that are more useful to you. Predefined views are provided to make things easier for you.

The pre-defined views are:

- **DeptView** - groups devices by their current department.
- **FirmwareView** - groups devices by their current firmware version.
- **GlobalView** - displays all devices without any sub-view.
- **ModelView** - groups all the devices by their model.
- **SandwichView** - groups devices after they are classified as part of a sandwich unit.

To change views:

- 1 Right-click with your cursor in the **DEVICE MANAGER**.
- 2 Select **Change View...**



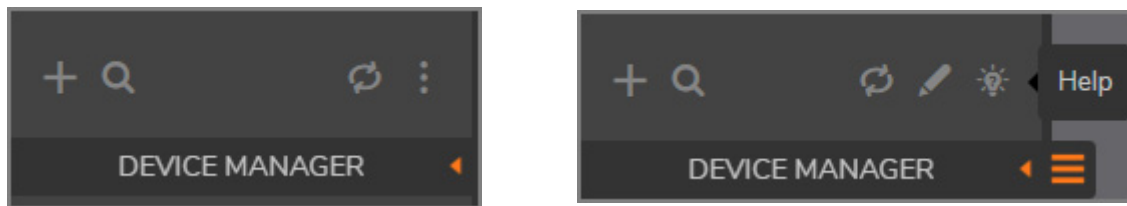
- 3 Select the view you want and click **OK**.

The following shows samples of the different views.



Using the Device Manager

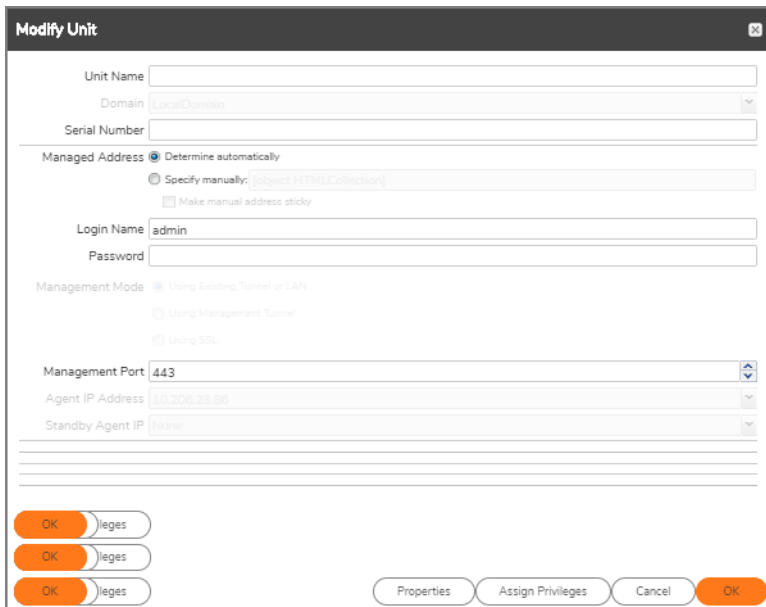
Use the icons above the **DEVICE MANAGER** to facilitate your work in this space.



- Click on the **Add Unit (+)** icon to add a firewall.
- Click on the **Search** icon to find a specific firewall in the list.
- Click on the **Reload Device Manager** icon to refresh the **DEVICE MANAGER**.

These options are available with configurations that include firewall management:

- Click on the vertical ellipsis icon to **Expand** your icon set.
- Click the **Edit** icon to **Modify a unit**.



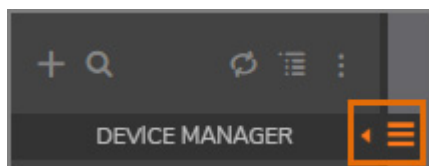
Additional information can be accessed by clicking on the devices names in the **DEVICE MANAGER**:

- Left-click on the device name and device information appears in the application work space.
- Right-click on the device name and additional commands are listed. Select an option to view or modify the settings.



Several of these same commands can be accessed using the icons at the top of the Device Manager panel.

The **DEVICE MANAGER** can be hidden by clicking on the orange **Show/Hide** icon.



Appliance Status

The status of the device is indicated by the colored symbols next to its name. Different symbols have different meaning, depending on configuration you are running. The generate definitions are:



Overview

The **HOME** view is the default view when you log in to GMS for the first time. This is where you can get a quick overview of status and reports for the devices in your infrastructure. Think of the **HOME** view as the starting point for most tasks.

Topics:

- [Status](#)
- [Dashboard](#)
- [Live Monitor](#)
- [Devices](#)

i **NOTE:** The commands available in the Overview section vary according to the Reporting Type you set when you installed GMS.

Status

The system goes through a series of steps when acquiring a firewall, and these steps can be monitored on the **Overview > Status** page, whether you use Zero Touch Deployment or manually bring it under management. The unit must first be plugged in for power and wired to both LAN and WAN for the device to be detected.

The Status page shows different things depending upon whether you have firewall management with Analytics or On-Premises Analytics, the Syslog-based option or IPFIX-based option. The interface shows which options are applicable to your implementation.

- [Acquisition History](#)
- [Firewall](#)
- [Network](#)
- [Management](#)
- [Reporting](#)
- [Subscription](#)
- [Firewall Information](#)
- [Fetch Information](#)
- [Synchronize with MySonicWall.com](#)
- [End User License Agreement](#)

Acquisition History

The steps taken while a unit is being acquired is tracked in the **Acquisition History** section of the **Status** page. As each stage is completed, success is indicated by a green check mark inside a small green box along with a message indicating status. If you want more information about each stage, you can expand it by clicking on the right arrow. More messages and status are displayed.

ACQUISITION HISTORY	
> UNIT SETUP	Success
> UNIT ACQUISITION	Success
> REPORTING AND ANALYTICS SETUP	Success
> FINISHED	Success

If an error occurs, or if a process seems to be taking too long, you can use the information from the expanded options to determine where to begin your troubleshooting. When the acquisition completes successfully, green check marks are shown for every stage.

NOTE: Acquisition History is not shown for On-Premises Analytics.

Firewall

The **Firewall** section of the **Status** page shows the data for the selected firewall. It provides information about the appliance model, registration status, serial number, domain, registration code, firmware version, CPU, and number of LAN IP addressed allowed.


FIREWALL	
Firewall Model	SonicWall SuperMassive 9400 North America
Firewall Registration Status	Registered
Serial Number	
Domain	LocalDomain
Registration Code	
Firmware Version	SonicOS Enhanced 6.5.2.2-40n - English
CPU	32 x 1200 MHz Mips64 Octeon Processor
High Availability	Disabled
Number of LAN IPs allowed	Unlimited


Network

The **Network** section of the Status page shows the physical interfaces available in the system that are up and running and those that are unassigned. It also displays the zones available and whether the DHCP Server is enabled or not. The symbols indicate the status of the interfaces. In the example, X0, X1, X2, X3, and X6 are available, but X4, X5, X7, X8, X9, X10, X11, X12, X13, X14, X15, X16, X17, X18, X19, U0, and U1 are unassigned. A green up arrow indicates the network interfaces are active and available. A yellow warning symbol indicates that there is a connection issue with those network interfaces. A red symbol means the interface is down

NETWORK

Interfaces

Physical  X0, X1, X2, X3, X6, MGMT

 X4, X5, X7, X8, X9, X10, X11, X12, X13, X14, X15, X16, X17, X18, X19, U0, U1


Zones LAN, WAN, DMZ, VPN, SSLVPN, MGMT, MULTICAST, WLAN, ZPD, WIRELESS-FRONT

DHCP Server Enabled

Management

The **Management** section of the **Status** page shows the management status for the selected firewall. A green up arrow indicates the firewall is online and connected.

MANAGEMENT

Firewall Status  since Jun 18, 2019 11:16:52 PDT

Firewall HA Status Unavailable


Unit added to SonicWall GMS on Jun 18, 2019 11:15:42 PDT

Management Mode SSL [10.206.27.134 : 443] (Manual)

Primary Agent SGMS 1 (10.206.23.86) (Active)

Standby Agent None

Tasks Pending No

Last Log Entry  Successful execution of task: Add New Bookm... [?](#)

SA Configuration Information

Defined SAs 3

Enabled SAs None

Available SAs 10050

Remaining SAs 10047

Interconnected SAs None

Reporting

The **Reporting** section of the **Status** page shows the current status of additional reporting services for the selected firewall.

REPORTING

Syslog Format Default

Status Messages Only Yes

Logs in UTC Yes

Analyzer Mode Enabled No

Name Resolution Mode DNS then NetBios

Subscription

The **Subscription** section of the **Status** page shows the current subscription status of all subscription services for the selected firewall.

SUBSCRIPTION	
VPN Upgrade	Yes
Global VPN Clients	Yes (2000)
Deep Packet Inspection for SSL (DPI-SSL)	Free Trial
Anti-Virus	
Gateway Anti-Virus, Anti-Spyware & Intrusion Preventio...	Current Jan 14, 2020
Content Filter List/Service	
Content Filtering Client	Expired [Nodes: 10] Jul 17, 2019
Premium Content Filter	Current Jan 14, 2020
Intrusion Prevention Service	
Gateway Anti-Virus, Anti-Spyware & Intrusion Preventio...	Current Jan 14, 2020
Capture Advanced Threat Protection	
Capture Advanced Threat Protection: Please visit MySon...	Current Mar 28, 2023
Gateway Anti-Virus, Anti-Spyware & Intrusion Preventio...	Current Jan 14, 2020
Support	
Software and Firmware Updates	Current Jan 14, 2020
Dynamic Support 24x7	Current Jan 14, 2020
Extended Warranty	Current Jan 14, 2020

Firewall Information

The **Firewall Information** section of the **Status** page shows the time since the selected firewall was last restarted and its firmware last modified.

FIREWALL INFORMATION AS OF 0 DAY, 4 HOURS, 59 MINUTES, 52 SECONDS BACK	
Firewall Up Time Since Last Reboot	3 Days, 11 Hours, 13 Minutes, 5 Seconds
Last Modified By	admin 10.206.23.86:X1 GMS UTC 08/20/2019 19:38:52

Fetch Information

The **Fetch Information** button of the **Status** page collects or refreshes current information for the selected firewall. This applies to Syslog-based implementations.

Synchronize with MySonicWall.com

SonicWall appliances check their licenses/subscriptions with MySonicWall once every 24 hours. You can manually synchronize with MySonicWall by clicking on the **Synchronize with MySonicWall.com** button if you want to synchronize immediately.

End User License Agreement

At the bottom of the Work Space, the **End User License Agreement** button provides the information specific to cloud implementations. It includes items such as SonicWall End User General Product Agreement, SonicWall Service Terms for Capture Security Center (Hosted Offering), and the End User License Agreement for SonicWall NS_v. Click on the button to learn more about end user product agreements and legal resources.

Dashboard

The **Dashboard**—located at **HOME > Overview > Dashboard**—provides a high-level view of the status of your security infrastructure. It summarizes the activity in easy-to-read, color-coded indicators. You can review the **Dashboard** and see at a glance if any issues need investigating.

NOTE: Syslog-based implementations do not display the **Dashboard**.



The **Dashboard** shows your devices and a representation of the traffic being generated. It allows you to view the devices in a geographical view using a map that you can zoom in and out of. The devices are marked on the map.

The following table describes the components that make up the Dashboard.

Dashboard

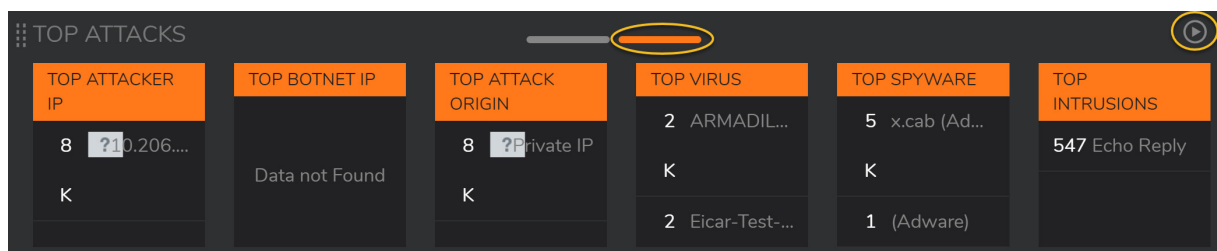
Feature	Description
Sliding bar and Custom button	At the top left, use the time-lapse sliding bar and the Custom button to customize the period for which the data is being shown. Use the sliding bar to select predefined periods or define a specific period by using the Custom option.
Export/Download, Refresh, and vertical More options icons	At the top right, use the icons to generate a flow report or download a Capture Threat Assessment, refresh the data, or see other options. The other options include viewing the Page Tips, going to Schedules (Reports Scheduled Reports > Schedules) or going to Archives (REPORTS Scheduled Reports > Archives) .
Totals	At the top of the table, totals are provided for your security infrastructure. It includes Total Connections, Total Data Transferred, Total Threats, and Total Blocked .
Risk Index	This bar graph indicates the level of risk your security infrastructure is currently exposed to. The values range from a single green bar to 10 bars with red meaning very high risk.
SYSTEM HEALTH/ TOP ATTACKS	<p>You can switch between the SYSTEM HEALTH (default) display and the TOP ATTACKS by clicking on the orange lines above the tiles. Switch between views . On the SYSTEM HEALTH view, the green tiles indicate the status of the options listed. Mouse over each tile to get more data. Click on the title of the tile to drill down for additional information. Depending on the feature, you are routed to Live Reports or a detailed report.</p> <p>The TOP ATTACKS cards show the features of top attacks. Mouse over the cards to get more details, and click on the tile title to drill down. When you click for more data, you are taken to REPORTS Details > [Tile_name].</p>
Threats Menu	At the right of the traffic map, the threats menu shows or hides information. This show/hide block focuses on THREATS, BLOCKED and TOP USERS . By clicking on these headings, you can jump to the detailed report for that topic heading (REPORTS Details > Topic_heading).
TRAFFIC MAP	<p>Displays the TRAFFIC MAP for your infrastructure. Switch between the WORLD VIEW and the GRID VIEW. On the WORLD VIEW, the threats are visually placed on the global map. you can use the roller on your mouse to zoom in or zoom out on a particular threat.</p> <p>The GRID VIEW shows the same traffic in table form, with additional details.</p>
TRAFFIC MAP Legend	Provides PRIVATE IP, FIREWALL, THREATS, INCOMING TRAFFIC, and OUTGOING TRAFFIC information.

SYSTEM HEALTH/TOP ATTACKS

Click on the tiles under **SYSTEM HEALTH** to drill down for more details. Some tiles take you to **Live Reports**, and others take you to the respective **Details** page; both are on the **REPORTS** view. Refer to *Analytics REPORTS Administration* for more information about these pages.

Mouse over the value in the tiles to see a tool tip that contains more information about the value.

You can toggle between the **System Health** tiles and the **Top Attacks** tiles. Click the gray bar above the tiles to switch to the other option. It turns to orange to show that it is the active view.



You can set the display so that it performs automatic switching between the **System Health** tiles and the **Top Attacks** tiles. Click the **Play** button in the upper right corner above the tiles. Click the **Pause** button if you want to turn off the switching.

TRAFFIC MAP

You can drill down for more information on the **TRAFFIC MAP** segment as well. Use the mouse wheel to Zoom in and out on the global map, or use the vertical **+** and **-** slider on the left side of the map. Click on the flags and icons on the map to drill down for more detail. If you would rather view a table version of the **WORLD VIEW**, click on the **GRID VIEW** icon above the map.

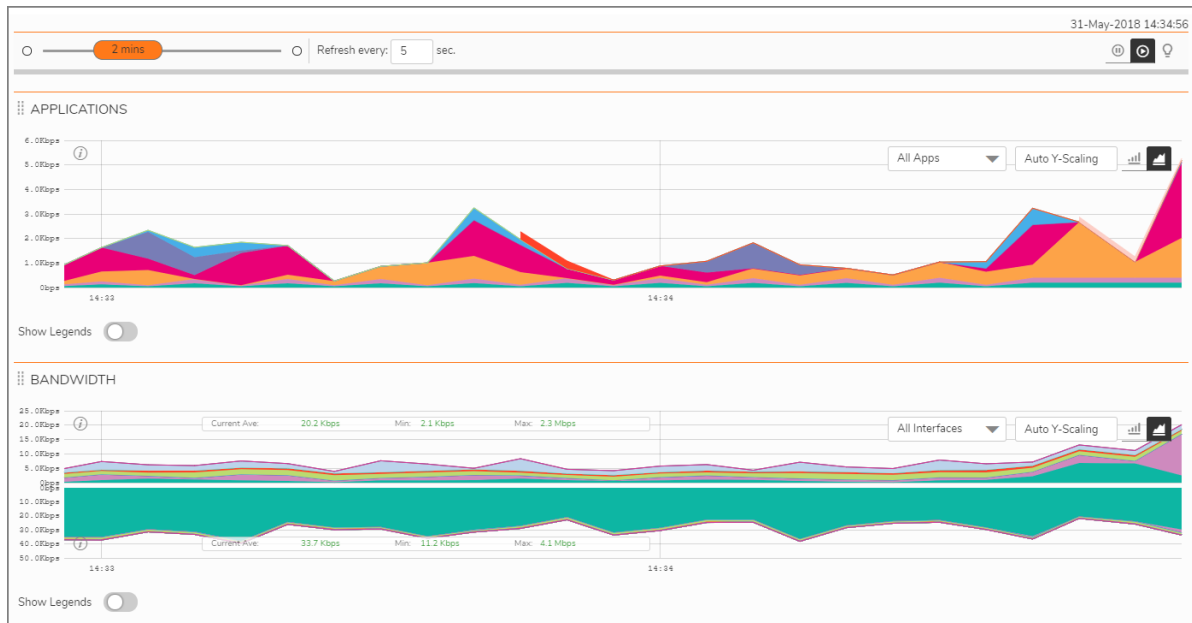
Dashboard Side Bar

The side bar beside the **TRAFFIC MAP** summarizes data for **THREATS**, **BLOCKED**, and **TOP USERS**. You can click on each line item in the side bar and you are taken to the associated Details report in the **REPORTS** view. (Refer to *Analytics REPORTS Administration* for more information about these pages.) Click on the Show/Hide icon to display or hide the side bar.

Live Monitor

Live Monitor provides a real-time view of the packets forwarded by the firewall and is visible when viewing and individual firewall. (If a group or **GlobalView** is selected in the **Device Manager**, the device options are shown instead.)

The **Live Monitor** is always running, but it does not store the data. After 10 minutes, the data is gone. However, while it is running, a background task is saving the data to a database. All data shown in Live Monitor is saved for historical reasons and you can find it in Live Reports (**REPORTS > Overview > Live Reports**).



Individual charts can be rearranged manually. Show or hide legends by clicking the **Show Legends** button.

The following charts are shown in **Live Reports**:

- **APPLICATIONS** indicates applications that are flowing through the firewall in bits per second.
- **BANDWIDTH** indicates the bandwidth utilization in bits per second.
- **PACKET RATE** shows average packets per second.
- **PACKET SIZE** shows average packets size.
- **CONNECTION RATE** indicates the new connection rate in connections per second.
- **CONNECTION COUNT** shows the total number of active connections.
- **MULTI-CORE MONITOR** shows the CPU utilization per core.

All the charts, except Connection Count, can be filtered to show a subset of the data. Click on the drop-down list in the chart and select the option you want. The chart clears and begins collecting data based on the new parameters.

To get details about the data being shown, mouse over the data in the graphs to see the value at that instant. The popup shows the details and the icons drilling down to get additional data. The icons take you to the following reports:

- Analytics (**ANALYTICS > All Traffic > Groups**)
- Graphs (**ANALYTICSC > All Traffic > Graphs**)
- Report view (**REPORTS > Details > report_type**, where *report_type* is the specific report found in the **Details** section)
- Sessions (**ANALYTICS > All Traffic > Session logs**)

Devices

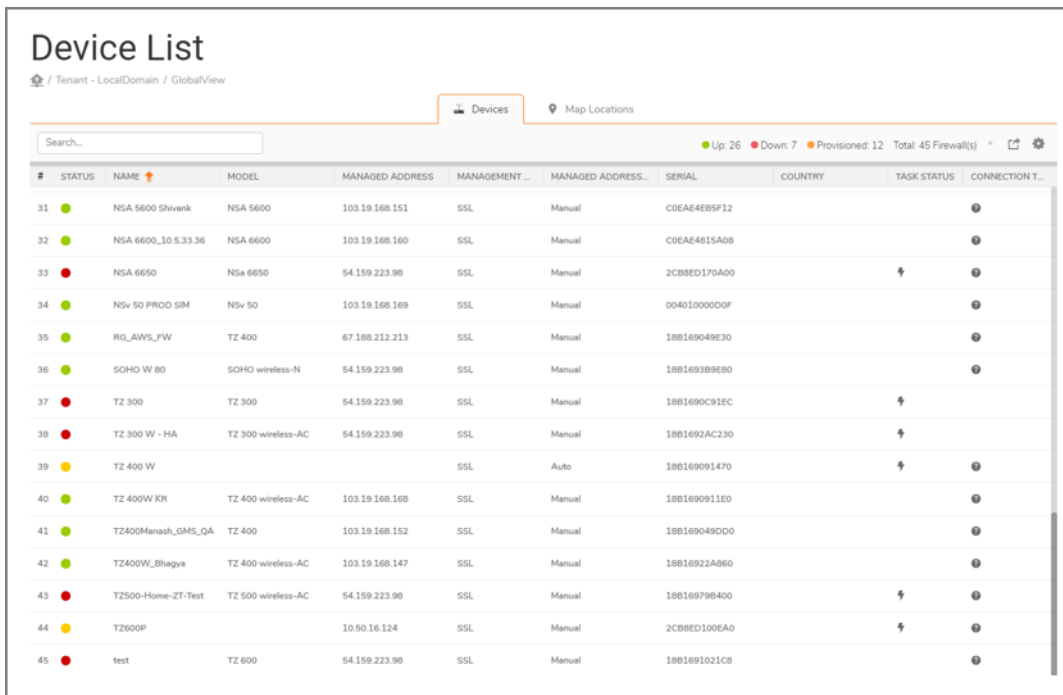
When you select **GroupView** or **GlobalView** in the **DEVICE MANAGER**, the **Live Monitor** option is not shown. You have the option to view your devices instead:

- For a CSC-MA implementation the menu option is **Device List**.
- For On-Premises Analytics, the menu option is **Devices**.

The functions for each are very similar.

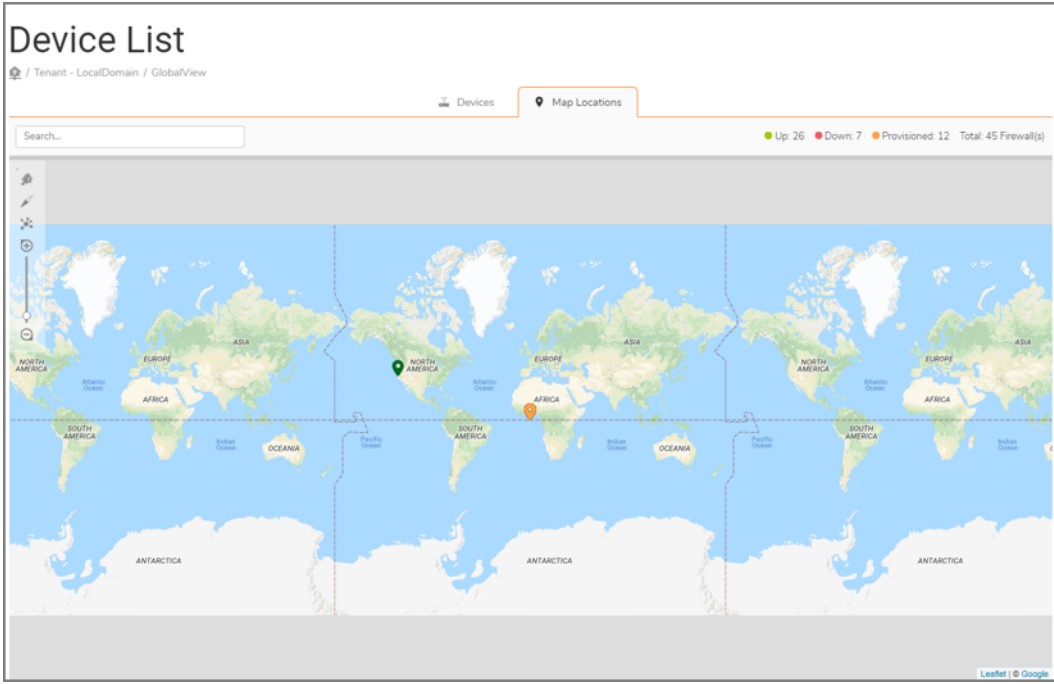
Device List

The following images show you the **Device List** for the group or global view you selected when in CSC-MA. The firewalls or virtual units that make up that view are listed in the table on the default view, which is the **Devices** tab. A summary showing the status of the devices in the group is shown at the top of the table. You can also search for a specific device to display, refresh the display or customize the table by using the search field and icons above the table.



#	STATUS	NAME	MODEL	MANAGED ADDRESS	MANAGEMENT	MANAGED ADDRESS...	SERIAL	COUNTRY	TASK STATUS	CONNECTION T...
31	●	NSA 5600 Shivank	NSA 5600	103.19.168.151	SSL	Manual	C0EAE4E85F12			🔍
32	●	NSA 6600_10 5.33.36	NSA 6600	103.19.168.160	SSL	Manual	C0EAE4815A08			🔍
33	●	NSA 6650	NSa 6650	54.159.223.98	SSL	Manual	2CB8ED170A00		🔍	🔍
34	●	NSv 50 PROD SIM	NSv 50	103.19.168.169	SSL	Manual	004010000D0F			🔍
35	●	RG_AWS_FW	TZ 400	67.188.212.213	SSL	Manual	18B169049E30			🔍
36	●	SOHO W 80	SOHO wireless-N	54.159.223.98	SSL	Manual	18B1693B9E80			🔍
37	●	TZ 300	TZ 300	54.159.223.98	SSL	Manual	18B1690C91EC		🔍	
38	●	TZ 300 W - HA	TZ 300 wireless-AC	54.159.223.98	SSL	Manual	18B1692AC230		🔍	
39	●	TZ 400 W			SSL	Auto	18B169091470		🔍	🔍
40	●	TZ 400W KR	TZ 400 wireless-AC	103.19.168.168	SSL	Manual	18B1690911E0			🔍
41	●	TZ400Manash_GMS_QA	TZ 400	103.19.168.152	SSL	Manual	18B169049D0D			🔍
42	●	TZ400W_Bhagya	TZ 400 wireless-AC	103.19.168.147	SSL	Manual	18B16922A860			🔍
43	●	TZ500-Home-ZT-Test	TZ 500 wireless-AC	54.159.223.98	SSL	Manual	18B169798400		🔍	🔍
44	●	TZ600P		10.50.16.124	SSL	Manual	2CB8ED100EA0		🔍	🔍
45	●	test	TZ 600	54.159.223.98	SSL	Manual	18B1691021C8			🔍

By selecting the **Map Locations** tab, you can see how the devices are distributed over a world map.



Devices

The following images show you **Devices** for the group or global view you selected while in On-Premises Analytics. The firewalls or virtual units that make up that view are listed in the table on the default view, which is the **Devices** tab. A summary showing the status of the devices in the group is shown at the top of the table. You can also search for a specific device to display, refresh the display or customize the table by using the search field and icons above the table.

Devices Device Groups

Search... Up: 2 Down: 0 Total: 2 Firewall(s)

#	FIREWALL	NAME ↑	SERIAL	MODEL	TRAFFIC
1	●	9400	COEAE48801BE	SuperMassive	↑
2	●	RG	COEAE40C2CF0	TZ	↑

Select the **Device Groups** tab to see the device groups that have defined for that set of devices. You can also define new groups on this page.


To create a new group:


- 1 Navigate to **HOME > Overview > Devices**.
- 2 Select the **Device Groups** tab.

- 3 Click the icon to **Create Device Group**.

CREATE A NEW FIREWALL GROUP ✕

Group Name

NAME 	SERIAL	MODEL
9400	C0EAE48801BE	SuperMassive
RG	C0EAE40C2CF0	TZ

NAME 	SERIAL	MODEL
No Data		

Close Save

- 4 Enter the **Group Name**.
- 5 Select the units and move them to the group.
- 6 Click **Save**.

Summary

The **Summary** reports provide various types of data being tracked for your security infrastructure. Think of these as executive summary reports that you can start with to check the general health for the topics listed. If an issue is reported, you can drill down from them.

 **NOTE:** Different options are shown in the **Summary** reports based on the options you licensed.

Topics:

- [Navigating the Summary Reports](#)
- [Applications](#)
- [Users](#)
- [Viruses](#)
- [Intrusions](#)
- [Spyware](#)
- [Web Categories](#)
- [Sources](#)
- [Destinations](#)
- [Source Locations](#)
- [Destination Locations](#)
- [BW Queues](#)
- [Botnet](#)
- [Blocked](#)
- [Threats](#)

Navigating the Summary Reports

You can customize and manage the data displayed in the **Summary** reports.

Topics:

- [Customizing Summary Reports](#)
- [Managing the Report Panels](#)

Customizing Summary Reports

At the top of the summary reports—no matter what topic you pick, you can customize and manage the reports displayed.

Option	Description
Sliding bar	Slide left or right to select a predefined period for the reports to cover. The default is 6 hours.
Custom option	Define a custom period for the reports to cover. Select starting and ending dates and times for the custom period.
Export/Downloads Options icon	Provides two options: <ul style="list-style-type: none">• Generate Flow Report PDF Generates a PDF document of the flow reports being displayed. The file is stored at REPORTS Scheduled Reports > Archive to download the report. The report may take several minutes to generate.• Download Capture Threat Assessment You must first download the Visualization Database for Offline Report Generation for your network traffic. This is a direct download to your file system. It is an .srf file that you upload to the CAT UI at MySonicWall. The PDF file is generated from that.
Refresh icon	Click on the Refresh icon at any time to refresh the data in these reports.
More vertical ellipsis icon	Click to access shortcuts for Pages Tips , Go to Schedules and Go to Archives .

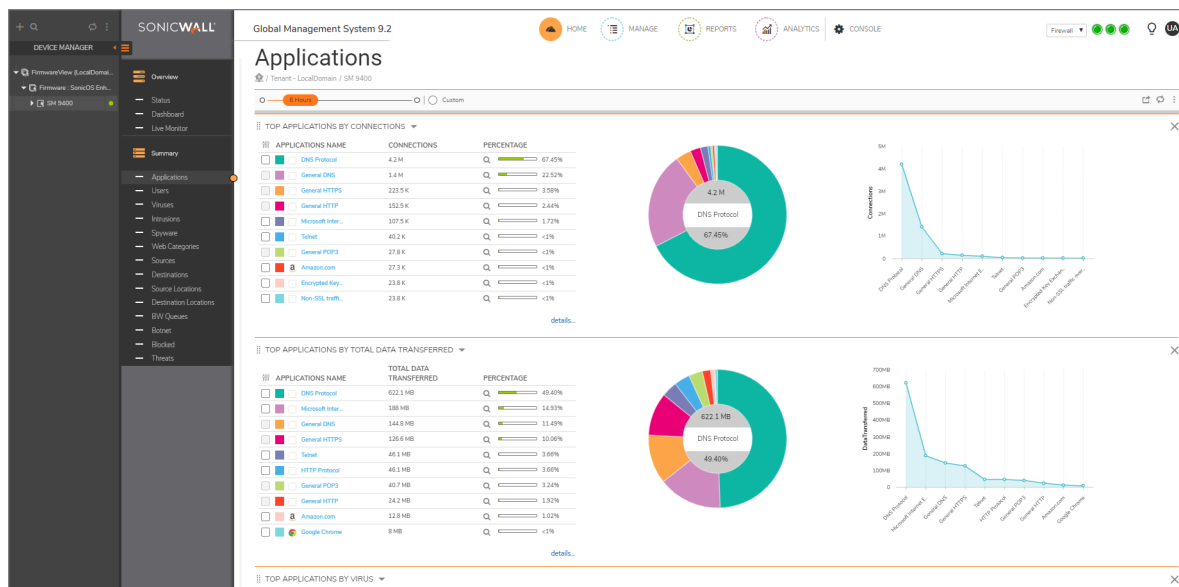
Managing the Report Panels

Once you select one of the topics under the Summary option, you can customize the reports shown.

Function	Description
To add predefined reports	<ol style="list-style-type: none">1 Click on the down arrow next to the report title.2 In the drop-down list, find the report you want to add.3 Click on the + sign and the new report is added to the bottom of the display.
To delete a report panel	Click on the X at the top right of the report panel.
To move a report panels	<ol style="list-style-type: none">1 Select and hold the icon to the left of the report title.2 Drag and drop the panel to the location that you want.

Applications

The Applications summary page has three types of reports displayed by default: **TOP APPLICATIONS BY CONNECTIONS**, **TOP APPLICATIONS BY TOTAL DATA TRANSFERRED**, and **TOP APPLICATION BY VIRUS**.



Additional application reports can be selected from the drop-down list by the title.

Top Applications by Connections	✓
Top Applications by Total data transferred	✓
Top Applications by Total connections blocked	+
Top Applications by Intrusions	+
Top Applications by Virus	✓
Top Applications by Spyware	+
Top Applications by Connections blocked by Botnet Filter	+
Top Applications by Connections blocked by Access Rule	+
Top Applications by Connections blocked by GeoIP Filter	+
Top Applications by Connections blocked by Threats	+
Top Applications by Connections blocked by CFS Service	+
Top Applications by Connections blocked by App Rule	+
Top Applications by Data Sent	+
Top Applications by Data Received	+

For Analytics in a cloud-based, firewall management, the **Applications** reports have multiple types. Choose the type you want from the tabs across the top of the table. They include **Applications**, **App Categories**, and **App Risk**. Reports for each tab can be selected from the drop-down list by the title.

Users

This report provides data at it relates to the users connected to the system. You can track user level transactions and activities by filtering on several different options.

Click on **HOME > Summary > Users** to see the application reports. **Top Users by Connections** and **Top Users by Total Data Transferred** are the two reports that are displayed by default. Additional user reports can be selected from the drop-down list by the title.

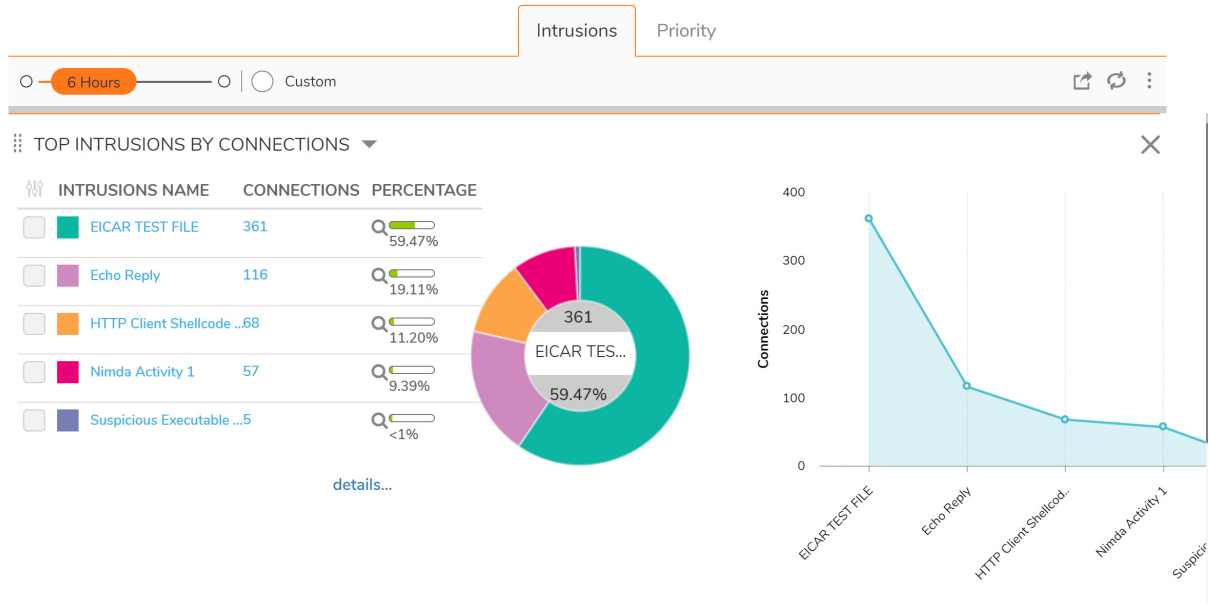
Top Users by Connections	✓
Top Users by Total data transferred	✓
Top Users by Total connections blocked	+
Top Users by Intrusions	+
Top Users by Virus	+
Top Users by Spyware	+
Top Users by Connections blocked by Botnet Filter	+
Top Users by Connections blocked by Access Rule	+
Top Users by Connections blocked by GeolP Filter	+
Top Users by Connections blocked by Threats	+
Top Users by Connections blocked by CFS Service	+
Top Users by Connections blocked by App Rule	+
Top Users by Data Sent	+
Top Users by Data Received	+

Viruses

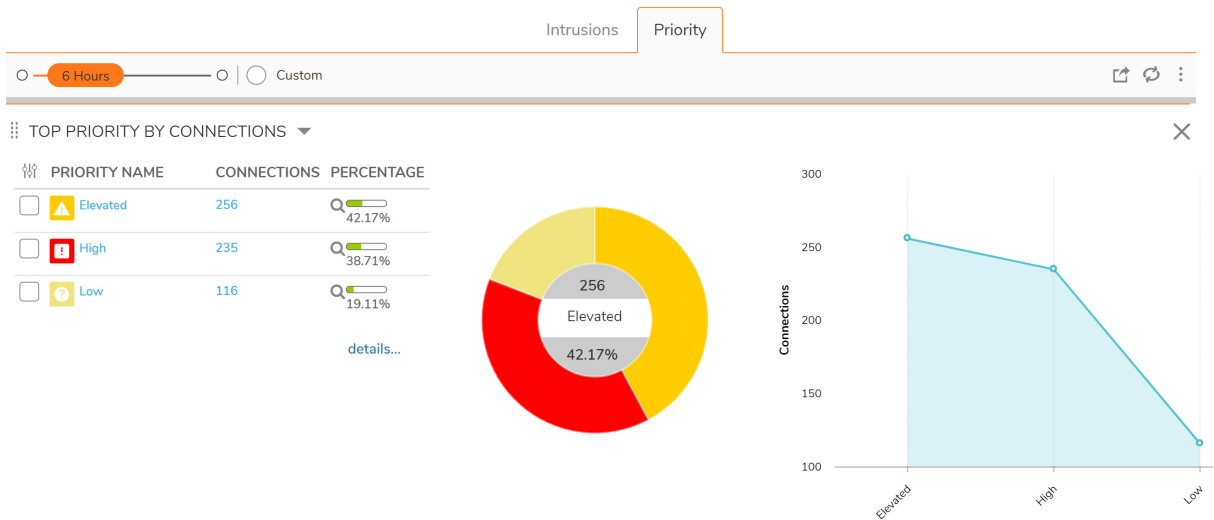
This report tracks the viruses that have been detected. You can filter on connections they occurred on or by which viruses were blocked. Details are provided in the table. Click on **HOME > Summary > Viruses** to see the viruses reports. Two reports are available and displayed by default: **Top Virus by Connections** and **Top Virus by Blocked**.

Intrusions

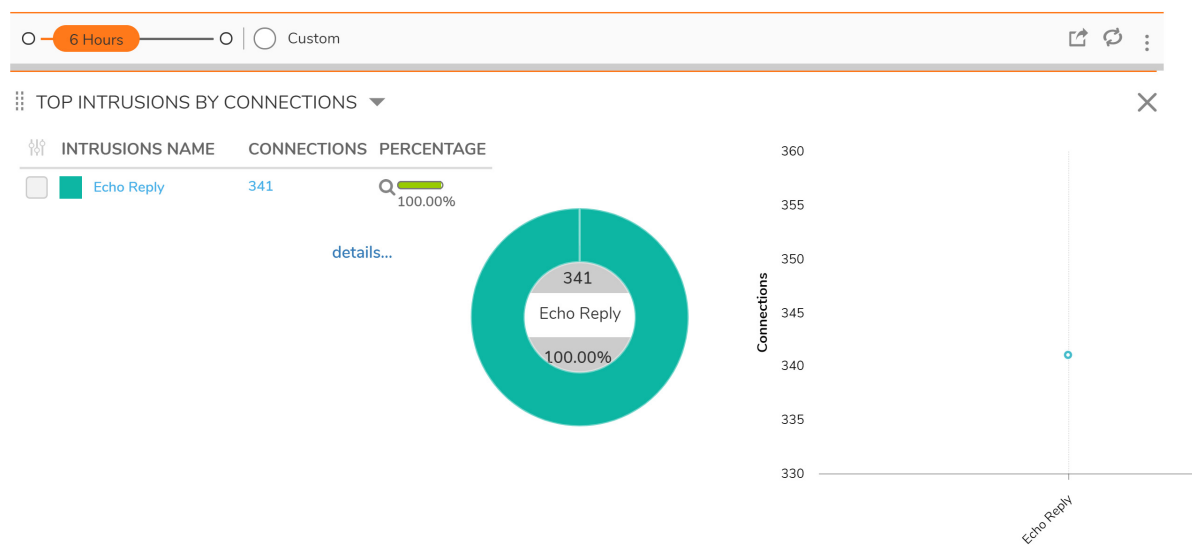
On the CSC-MA system, the Intrusions summary has two types of reports (represented by the different tabs): **Intrusions** and **Priority**.



The **Priority** tab is only visible on CSC-MA, and it show the top priority intrusions by connections and by blocked. Select the **Priority** tab.



Some configurations only have a single view for **Intrusions**.



This report tracks the intrusions that have been detected. You can filter on the connections they occurred on or by which intrusions were blocked. Details are provided in the table. Click on **HOME > Summary > Intrusions** to see the intrusion reports. Two reports are available and displayed by default: **Top Intrusions by Connections** and **Top Intrusions by Blocked**.

Spyware

This report tracks the spyware that has been detected. You can filter on connections they occurred on or by which spyware was blocked. Details are provided in the table. Click on **HOME > Summary > Spyware** to see the intrusion reports. Two summary reports are available and displayed by default: **Top Spyware by Connections** and **Top Spyware by Blocked**.

Botnet

This report tracks the Botnet addresses that are detected. Click on **HOME > Summary > Botnet** to see the **Botnet** report. Only one summary report is available and displayed by default: **Top Botnet by Connections**.

Web Categories

On the CSC-MA system, the Web Categories summary has two types of reports (represented by the different tabs): **Web Categories** and **Websites**. The on-premises Analytics one has a single view for **Web Categories**.

This report displays the number of connections based on web categories. You can filter on the categories in the **View** drop-down list. Details are provided in the table. Click on **HOME > Summary > Web Categories** to see the web categories report. Two summary reports are available and displayed by default: **Top Web Categories by Connections** and **Top Web Categories by Total Data Transferred**. The reports can be selected from the drop-down list by both titles. There is only one report for On-Premises Analytics.

Top Web Categories by Connections	✓
Top Web Categories by Total data transferred	✓
Top Web Categories by Total connections blocked	+
Top Web Categories by Blocked	+
Top Web Categories by Spyware	+
Top Web Categories by Virus	+
Top Web Categories by Intrusions	+
Top Web Categories by Connections blocked by Access Rule	+
Top Web Categories by Connections blocked by GeolP Filter	+
Top Web Categories by Connections blocked by Botnet Filter	+
Top Web Categories by Connections blocked by CFS Service	+
Top Web Categories by Connections blocked by App Rule	+

Sources

This report displays the number of connections based on IP address of the source. You can filter on the IP addresses listed in the **View** drop-down list or on other options listed in the **By** drop-down list. Details are provided in the table. Click on **HOME > Summary > Sources** to see the source IP reports. Two summary reports are available and displayed by default: **Top Initiator IPs by Connections** and **Top Initiator IPs by Total Data Transferred**. Additional source IP reports can be selected from the drop-down list by the title.

Top Initiator IPs by Connections	✓
Top Initiator IPs by Total data transferred	✓
Top Initiator IPs by Total connections blocked	+
Top Initiator IPs by Intrusions	+
Top Initiator IPs by Virus	+
Top Initiator IPs by Spyware	+
Top Initiator IPs by Connections blocked by Botnet Filter	+
Top Initiator IPs by Connections blocked by Access Rule	+
Top Initiator IPs by Connections blocked by GeolP Filter	+
Top Initiator IPs by Connections blocked by Threats	+
Top Initiator IPs by Connections blocked by CFS Service	+
Top Initiator IPs by Connections blocked by App Rule	+
Top Initiator IPs by Data Sent	+
Top Initiator IPs by Data Received	+

Destinations

This report displays the number of connections based on IP address of the source. You can filter on the source type listed in the **View** drop-down list or on other options listed in the **By** drop-down list. Details are provided in the table. Click on **HOME > Summary > Destinations** to see the destination IP reports. Two reports are available and displayed by default: **Top Responder IPs by Connections** and **Top Responder IPs by Total Data Transferred**. Additional destination IP reports can be selected from the drop-down list by the title.

Top Responder IPs by Connections	✓
Top Responder IPs by Total data transferred	✓
Top Responder IPs by Total connections blocked	+
Top Responder IPs by Intrusions	+
Top Responder IPs by Virus	+
Top Responder IPs by Spyware	+
Top Responder IPs by Connections blocked by Botnet Filter	+
Top Responder IPs by Connections blocked by Access Rule	+
Top Responder IPs by Connections blocked by GeolP Filter	+
Top Responder IPs by Connections blocked by Threats	+
Top Responder IPs by Connections blocked by CFS Service	+
Top Responder IPs by Connections blocked by App Rule	+
Top Responder IPs by Data Sent	+
Top Responder IPs by Data Received	+

Source Locations

This report displays the number of connections based on location of the source. You can filter on the connection type listed in the **View** drop-down list or on other options listed in the **By** drop-down list. Details are provided in the table. Click on **HOME > Summary > Source Locations** to see the source location reports. Two reports are available and displayed by default: **Top Initiator Locations by Connections** and **Top Initiator Locations by Total Data Transferred**. Additional source IP reports can be selected from the drop-down list by the title.

Top Initiator Locations by Connections	✓
Top Initiator Locations by Total data transferred	✓
Top Initiator Locations by Data Sent	+
Top Initiator Locations by Data Received	+
Top Initiator Locations by Connections blocked by GeolP Filter	+

Destination Locations

This report displays the number of connections based on country of the destination. You can filter on the locations listed in the **View** drop-down list or on other options listed in the **By** drop-down list. Details are provided in the table. Click on **HOME > Summary > Destination Locations** to see the destination location reports. Two reports are available and displayed by default: **Top Responder Locations by Connections** and **Top Responder Locations by Total Data Transferred**. Additional destination IP reports can be selected from the drop-down list by the title.

Top Responder Locations by Connections	✓
Top Responder Locations by Total data transferred	✓
Top Responder Locations by Data Sent	+
Top Responder Locations by Data Received	+
Top Responder Locations by Connections blocked by GeoIP Filter	+

BW Queues

This report tracks the bandwidth data. The default is the **Inbound Realtime** view, but you can choose the **Outbound Realtime** view from the View drop-down list. You can also filter on other options listed in the **By** drop-down list. Data for both views are shown in the table. Click on **HOME > Summary > BW Queues** to see the various bandwidth management reports. Two reports are available and displayed by default: **Top Bandwidth Management by Connections** and **Top Bandwidth Management by Total Data Transferred**. Additional destination reports can be selected from the drop-down list by the title.

Top Bandwidth Management by Connections	✓
Top Bandwidth Management by Total data transferred	✓
Top Bandwidth Management by Data Sent	+
Top Bandwidth Management by Data Received	+

Blocked

This report tracks the number of blocked connections. The default view is **Total**, but you can select **Threats** or **Botnet** from the View drop-down list. Data for both options are shown in the table. Click on **HOME > Summary > Blocked** to see the blocked threats report. Only one summary report is available for Blocked: **Top Blocked by Connections**.

Threats

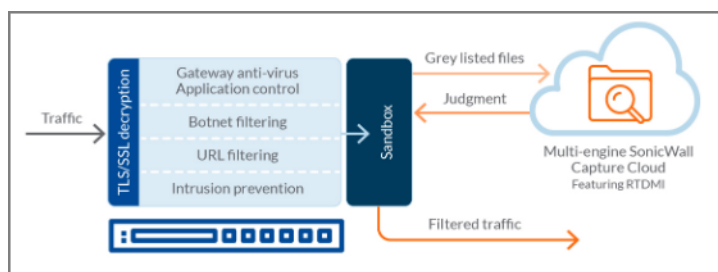
This report tracks the number of connections with threats. The default view is **Total**, but you can select **Intrusions** or **Virus** from the View drop-down list. You can also filter on other options listed in the **By** drop-down list. Details are shown in the table. Click on **HOME > Summary > Threats** to see the threats reports. Two reports are available and displayed by default: **Top Threats by Connections** and **Top Threats by Blocked**.

Customizing and navigating the reports is summarized in [Navigating the Summary Reports](#).

Capture ATP

The **SonicWall Capture Advanced Threat Protection (ATP)** section of the **HOME** view provides a cloud-based network sandbox that analyzes suspicious code. By doing so, it helps to discover and stop ransomware, advanced persistent threats (APTs), and zero-day attacks from entering the network at the gateway until a verdict is determined. It displays the status of the firmware being used to send files to the backend for protection.

Capture ATP offers multi-layer sandboxing; including SonicWall's Real-Time Deep Memory Inspection (RTDMI), full system emulation and virtualization techniques, to analyze suspicious code behavior. It scans traffic, suspicious code, and a broad range of file sizes and types.



Status

The **Status** section lets you know which files are sent to the backend for scanning and which ones are blocked. The blue box shows the total files scanned and the red box shows the total malicious files found. Files are scanned for the last 30 days.

It also informs you about the date of the work being done by the firewall and how many files have been scanned. Colored bars on the status report at the top right give you the percentage and number of days of malicious files found.

Status reports are available in this section. You can add filters to the files being scanned and see the files by their name, submitter, and the source and destination IP addresses.

For more information, refer to the SonicWall Management Services Capture ATP Administration Guide.

NOTE: Capture ATP is an add-on security service to the firewall, similar to Gateway Anti-Virus (GAV), that helps your system identify malicious files. To enable the service you need a license, GAV, and Cloud Anti-Virus Database services.

SonicWall Analytics

HOME | REPORTS | ANALYTICS | NOTIFICATIONS | CONSOLE

Status

9400

Capture ATP - Status

TOTAL FILES SCANNED: 110671 | MALICIOUS FILES: 7762

FILES SCANNED IN THE LAST 30 DAYS

VIEWING 110671 FILES SCANNED

STATUS	FILENAME	DATE	SOURCE	DESTINATION	COUNTRY	TOTAL BYTES
scan pending	3dEggs.exe.bin	Mar 29 - 4:15pm	10.206.27.196:80	192.168.168.20:35955	Private IP	358.21K
scan pending	3dEggs.exe.bin	Mar 29 - 4:15pm	10.206.27.196:80	192.168.168.20:35953	Private IP	347.26K
scan pending	3dEggs.exe.bin	Mar 29 - 4:14pm	10.206.27.196:80	192.168.168.20:35952	Private IP	291.75K
scan pending	3dEggs.exe.bin	Mar 29 - 4:14pm	10.206.27.196:80	192.168.168.20:35951	Private IP	299.19K

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 HOME Administration
Updated - October 2019
232-005147-00 Rev A

Copyright © 2019 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

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