SonicWall® Analytics NOTIFICATIONS

Administration

SONICWALL®

Contents

1

About Notifications

NOTIFICATIONS is featured on IPFIX-based, cloud-based Analytics solutions. It allows administrators and users:

- To see the **Status** of their firewall network system
- To set **Rules** for their firewall network system
- To see the **History** of the rules that hit their rules and notifications

NOTE: The interface for Analytics varies because of the different configurations and types of reporting that can be set up. 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.

Topics:

Understanding NOTIFICATIONS

When your on-premises system is connected to a firewall, the data flows from the firewall to your on-premises appliance. However, when you connect your on-premises system to the CSC-MA solution, the **NOTIFICATIONS** feature is displayed on your on-premises device.

Remember you can only access the **NOTIFICATIONS** feature if your on-premises/firewall system has been integrated with a SonicWall cloud-based, firewall management system. If you have not integrated your on-premises/firewall system with the CSC-MA license, your view is different than the blended implementation of the on-premises/firewall system.

The data for your on-premises system is on the on-premises server and not on the CSC-MA system. You need the App Visualization license for the visualization and flow reporting services on the CSC-MA. This license is included with the existing GAV/IPS, AGSS or CGSS and Total Secure licenses.

NOTE: The **NOTIFICATIONS** option is not available for all Analytics implementations. The **NOTIFICATIONS** icon shows with the top navigation icons if you have the proper licenses and implementation.

Accessing NOTIFICATIONS

When you select the **NOTIFICATIONS** view, the default view is **NOTIFICATIONS| Alerts & Notifications > Status**. The **Status** page is the starting point to receive all the alerts and notifications triggered using data flow and incorporating the analytics framework.

NOTE: The same Status page can be seen by navigating to **HOME > Overview > Status**.

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

Device Manager	In the **DEVICE MANAGER**, you can group the devices in your security infrastructure using the pre-defined views.
Command menu	The command menu is located directly under the SonicWall logo. You can manage or monitor your devices using the commands shown here.
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.

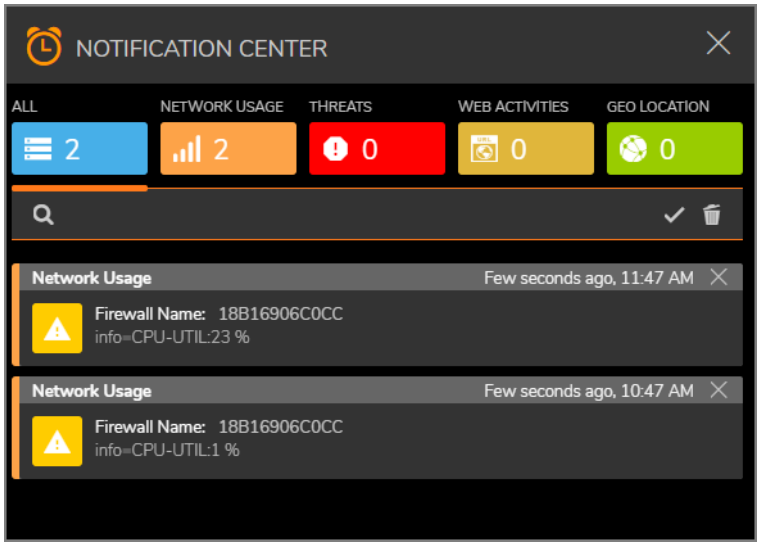
For more information about using the Analytics interface, refer to “Navigation” in *Analytics HOME Administration*.

Notification Center

The Notification Center is not specifically part of the **NOTIFICATIONS** view, but is a separate view that provides the status and activities being monitored and recorded by Analytics. After clicking on the Alerts and Notifications icon at the top of the interface, 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.

Individual alert messages arrive and are displayed in the body of the Notification Center. They are triggered based on how the alerts are defined in the Rules. The individual messages show the alert name, the firewall name, and the time they are triggered at. They are listed in the order they arrive. They have a priority of high, medium, and low in terms of severity.



In the search bar, you can search by firewall name, alert name, message or details. Clear your search by clicking on the **X** to the right of the search text you typed.

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 a 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.

Related Documents

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

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

2

Status

The system goes through a series of steps when acquiring a firewall. These steps can be monitored on the **NOTIFICATIONS | Alerts & Notifications > Status** page when you log in to Capture Security Center-Management and Analytics (CSC-MA) and on-premises Analytics.

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.

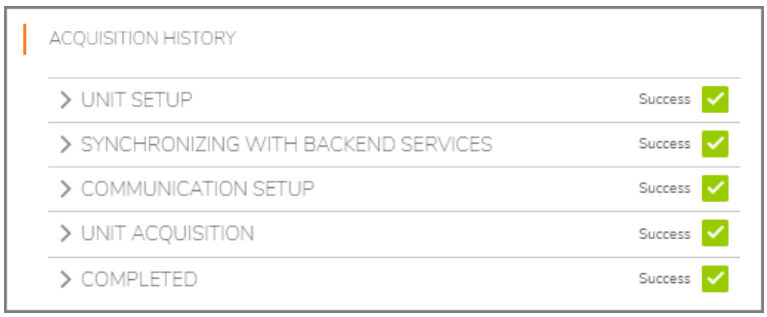
IMPORTANT: Zero Touch is not supported with CSC-MA when implemented with on-premises Analytics.

NOTE: The commands in the Command Menu vary according to the type of view you choose in the Device Manager. Differences are noted when applicable.

Topics:

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.

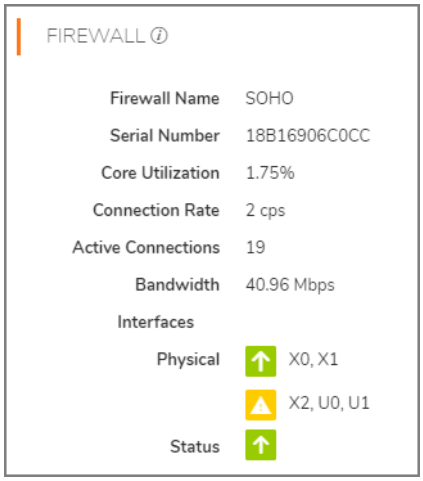


If an error occurs, or if a process seems to be taking too long, you can use the information from the expanded options to determine where to begin your troubleshooting. When the acquisition completes successfully, green check marks are shown for every stage.

NOTE: Acquisition History is not shown for on-premises Analytics.

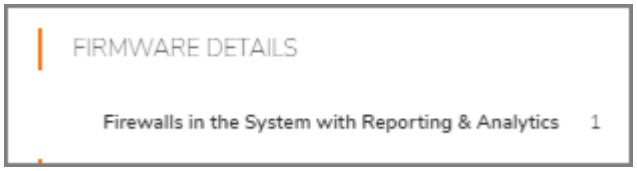
Firewall

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, CPO, and number of LAN IP addressed allowed.



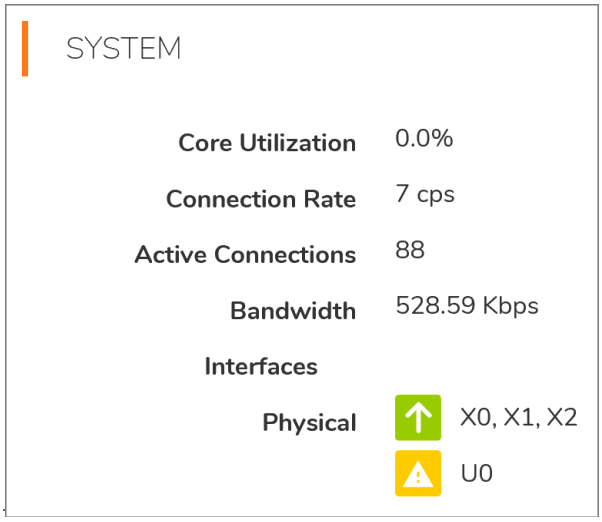
Firmware Details

The **Firmware Details** section of the Status page, for CSC-MA, shows the data for the selected firewall.



System

The **System** section of the **Status** page shows the system and interface data for the selected firewall. The following shows a sample:

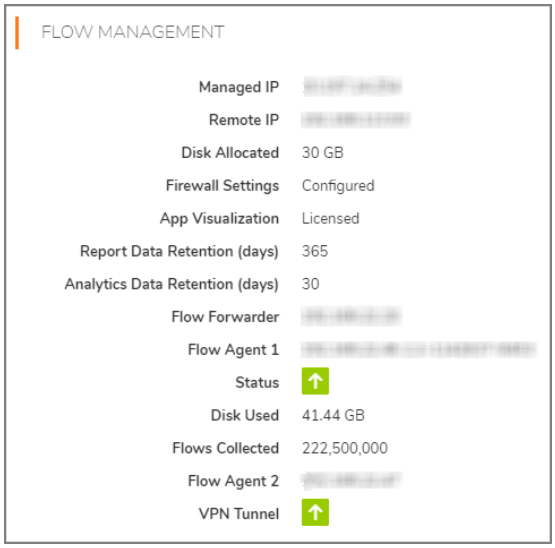


The symbols indicate the status of the interfaces. In the example, X0, X1, and X2 are available, but U0 is unassigned. This section also shows the status of virtual interfaces, when present. A red symbol means the interface is down.

Flow Management

The **Flow Management** section of the **Status** page shows statistics about the flow agent you set up on this device. The **Flow Management** section for on-premises Analytics provides a smaller set of information than the CSC-MA Analytics.

NOTE: If the VPN Tunnel is down, the Status field appears and provides a message describing what the issue might be. You can use this information to begin your troubleshooting.



The green arrow symbol means that the VPN tunnel was successfully established.

Flow Reporting License Status

The **Flow Reporting License Status** section of the **Status** page shows whether you have the license for the provided flows that traverse the firewall. The AFM and RTM should start showing data visualizing these flows in a real-time fashion.

Adding and Deleting Firewalls

The **Adding and Deleting Firewalls** section of the **Status** page provides the steps for adding the device to your system.

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.

3

Rules

You can create customized alerts and notifications to notify you of the things you are most concerned with. Once you create your alerts and notifications, you can archive them and preserve them across restarts, backups and restores.

Navigate to **NOTIFICATIONS > Alerts & Notifications > Rules**.

The **Rules** view is broken into the following sections:

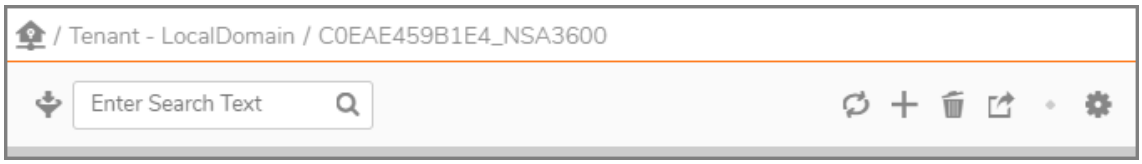
- Navigating the Rules
- Managing the Rules

Navigating the Rules

Think of the **Rules** view as the place where you can set behaviors for your firewall to follow. The **Rules** include valuable notifications and network alerts that you can define to extend or override default rules. For example, you can create an alert to specifically block certain types of traffic such as violence, hate, or racism. You can also allow certain types of traffic, such as government or information technology.

You can also prevent damaging data containing computer viruses from entering your security network. These important rules evaluate network traffic sources and compare the information against the rules you have created.

NOTE: For one firewall, you can set one rule per alert type.

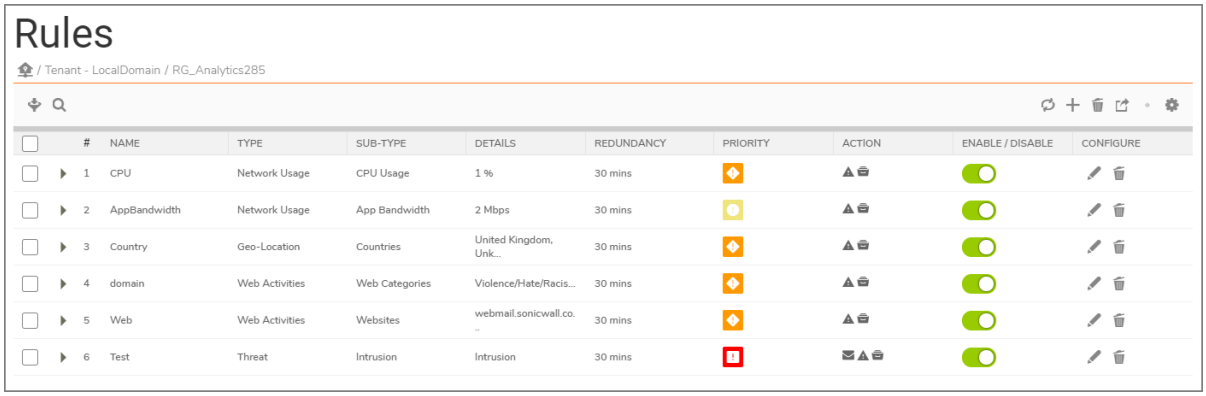


Rules Options

Option	Description
Tenant	Displays the tenant or domain for your network that includes its users, servers, appliances, and so forth.
Filter	Allows you to sort by alert priority, type, and sub-type.
Search	Allows you to enter search text to find your data.
Refresh	Refreshes the data in the reports.
Add	Allows you to add an alert.
Delete	Deletes one or more selected alerts.
Export/Download	Exports the data directly from grid view to a CSV file and download it.
Show/Hide	Select table columns to show or hide to customize your view.

You can set up four types of alerts: **Network Usage**, **Threat**, **Web Activities**, and **Geo-Location**. For any alert, you can set **Rules**, configure its **Settings** and its **History**. You can set one of the latter configurations or all of them for your rule.

NOTE: You can only set your alerts at the firewall unit level.



Rules Alerts

Rules	Description
NAME	The name of the rule
TYPE	The kind or group of your alert rule
SUB-TYPE	The sub-type of your broader alert rule
DETAILS	Additional details related to your alert rule
REDUNDANCY	How often the alert repeats
PRIORITY	The importance you assigned to the alert rule
ACTION	The actions you associated with the alert rule
ENABLE / DISABLE	Where you turn the rule on and off
CONFIGURE	Where you can edit or delete a rule

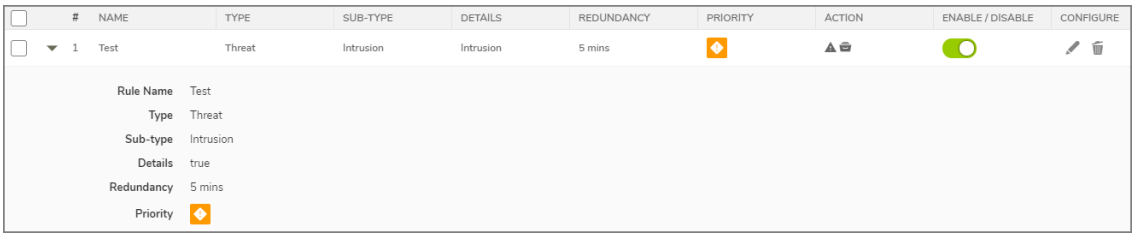
Alert Check Box, Details, and Number

The first three columns in the **Rules** table, at the top left, help you select and expand your alerts by clicking on the empty check boxes, the right caret signs, and identifying them by their given index numbers.

Using the selection and expansion alert columns:

1 Click the check box to highlight your alert. Your selection is indicated by an orange check mark.

2 Click the right caret sign to expand the alert and get more details.

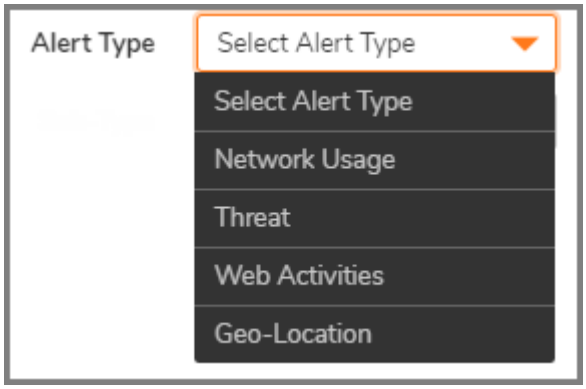


Alert Name

You can choose any name you want for your alert. There is no limit as to the number of characters your alert name can have. An orange up and down arrow, next to the column name, indicates you can sort your alert names in ascending or descending order.

Alert Type

You can choose from four types of alerts: **Network Usage**, **Threat**, **Web Activities**, and **Geo-Location**. Refer to the image and table below for more information about alert types. An orange up and down arrow, next to the column name, indicates you can sort your alert type in ascending or descending order.



Alert	Description
Network Usage	The amount of data sent and received by your network.
Threat	The potential malware that could cause serious harm to your network. You can configure which threat alert type to monitor. If there is a threat detected, a notification is sent with additional information. For example, for Botnet, the additional information is the IP address which is suspected to be a Botnet. For Intrusion, Spyware and Virus, the extra information is the name of the malware or threat.

Alert	Description
Web Activities	The web activities in real time taking place in your network, including analysis of IP addresses, website names, etc.
Geo-Location	The identification or estimate of the real-world geographic location of the web activities, web-related traffic, and web connected computer terminals being used or occurring in your network. An alert is set for an initiator country, responder country, or both. If there is a hit, a notification is sent with additional information on the country, IP address, etc.

Alert Sub-Type

You can work with different alert sub-types depending on the alert type you choose. You have to toggle to enable the alert sub-type or take some extra steps once you are adding your alert. Refer to the table below for more information about alert sub-types. An orange up and down arrow, next to the column name, indicates you can sort your alert sub-type in ascending or descending order.

Alert	Alert Sub-Type
Network Usage	• **App Bandwidth:** the capacity to transfer data in your network security system and its rate threshold. • **Interface Bandwidth:** the inherited and received bandwidth for an interface rate threshold. • **Max Connection Count:** the maximum number of open HTTP connections and its usage count threshold. • **CPU Usage:** how much the central processing unit is working and its usage percentage threshold. • **Per Interface:** the interface connection rate, packet rate and bandwidth thresholds.
Threat	• **Botnet:** The number of internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack) steal data, send spam, and allow the attacker to access the device and its connection. • **Intrusion:** the identification and detection of malicious data and activity. • **Spyware:** the identification and detection of malicious data and activity that puts at risk logins, passwords, and network details. • **Virus:** a piece of code which can copy itself and typically has a detrimental effect, such as corrupting your network security system and destroying your data.
Web Activities	• **Websites:** the group of web pages containing hyperlinks made available online by different entities. • **Web Categories:** the distinct types to which the websites belong to.
Geo-Location	• **Countries:** the different geographic areas where the alert is set for an initiator country, responder country, or both.

Alert Details

Your alert **DETAILS** depend on the alert type and sub-type that you choose. Refer to the table below to learn about the details for each alert.

Alert Type	Details
Details	The alert attributes that are displayed in the Rules table when you click on the side caret key.
Email Groups	The email address used to send messages electronically to a group.

Alert Type	Details
Email Address	The email address used to send messages electronically to a person or a single entity.
Archive Days	The time your data is preserved and saved in the network.

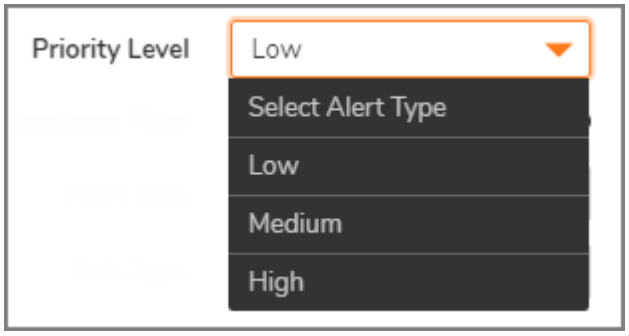
Alert Redundancy Filter

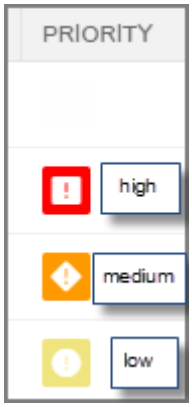
To get high quality alerts and avoid false positives, CSC has a filter that helps sift out and reduce redundant alerts. The filter restricts the number of identical log entries to a specific number per second and up to six hours. For example, if the log redundancy filter is configured with a value of 30 seconds on the time sliding bar, CSC creates duplicate log entries every 30 seconds.

The alert redundancy filter has a default setting of two minutes and the alert redundancy filter for threats has a default setting of five minutes. An orange up and down arrow, next to the column name, indicates you can sort your alert redundancy filter in ascending or descending order.

Alert Priority Level

The alert priority level assigns a severity level to the rule. The level is precise to avoid a false positive. There are three priority levels: **Low**, **Medium**, and **High**. For example, if you decide that a particular alert needs a higher priority, all you have to do is increase its severity to the higher priority levels. An orange up and down arrow, next to the column name, indicates you can sort your alert priority in ascending or descending order.





Alert Notification Actions

When the conditions of an alert rule matches, a notification action is sent. The following are the available actions to take:

- Log to Archive
- Email
- System Alert Message

Log to Archive is the default. This should always be set. An alert can be sent to a specific email address or a specific email address for a group.

Notifications can also be sent to **System Alert Message** in the Console. No matter which page view the user or administrator has, notifications with this setting show up as a System Alert messages.

The actions you take on an alert are indicated under the **ACTION** column by three possible symbols. From left, the three symbols in the image below indicate the following:

- Mail icon: the alert is configured with an email address.
- System alert icon: the system alert message is enabled.
- Archive icon: the alert is archived.

Managing the Rules

You can take several actions on the rules. This section describes each of them:

- Enabling Alerts
- Adding an Alert
- Editing an Alert Rule
- Alert Sub-Types
- Deleting an Alert

Enabling Alerts

To enable or disable your alerts from the Rules table:

1 Under the **ENABLE / DISABLE** column, toggle your choice.

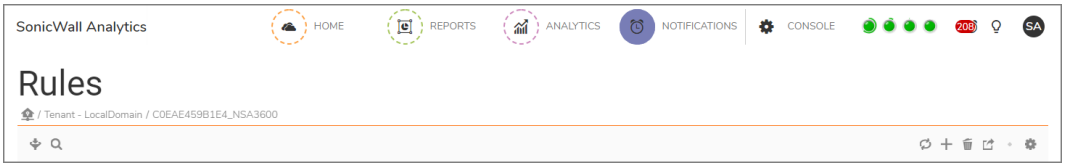
A small dialog box displays at the top of the work space asking you to confirm your selection.

2 Click **OK** to save the change or **Cancel** to retain the old setting.

Adding an Alert

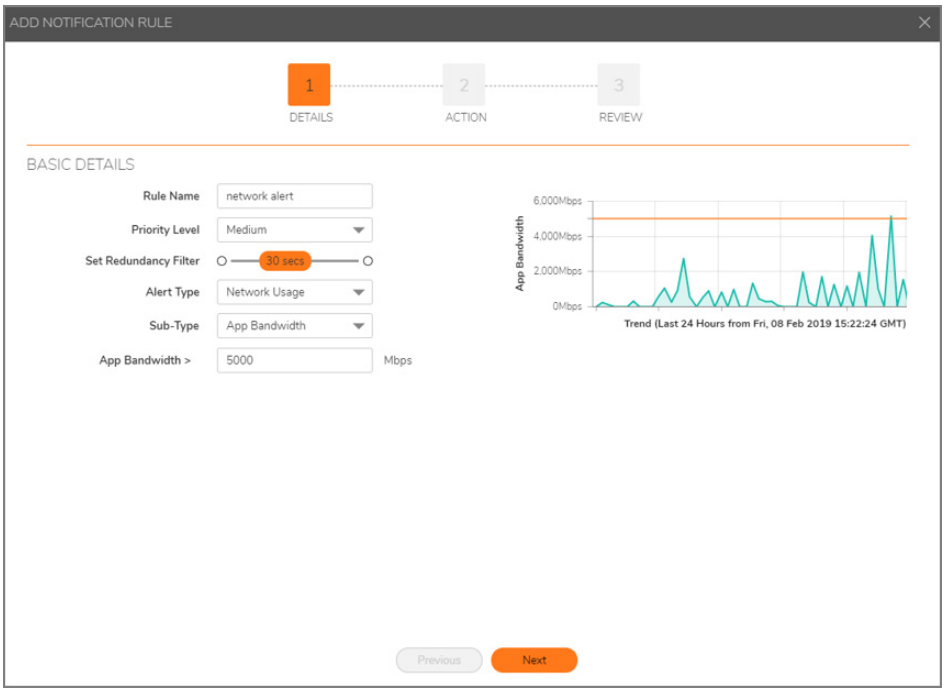
To add an alert:

1 On the left navigation panel, navigate to **Alerts & Notifications > Rules** to see the Rules table with its commands on top.



2 Click the **+ Add Alert Rule** icon to add an alert.

The **ADD NOTIFICATION RULE** dialog box displays. This view is indicated by the orange square icon with the number 1 inside.



3 Enter the name of the rule next to **Rule Name**.

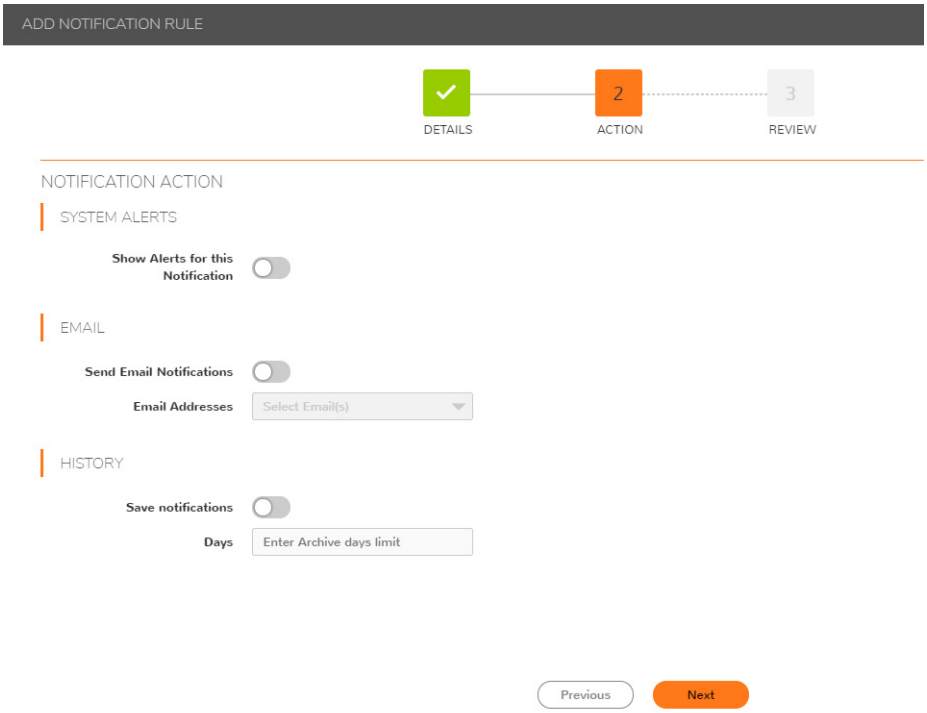
4 Select the rule **Priority Level** from the drop-down menu choices, which are **Low**, **Medium**, and **High**.

5 Click the time slider, next to **Set Redundancy Filter**, to choose your desired frequency.

6 Select the **Alert Type** from the drop-down menu choices. The choices are **Network Usage**, **Threat**, **Web Activities**, and **Geo-Location**.

7 Select the alert **Sub-Type** from the drop-down menu choices. The options listed depend on the **Alert Type** you choose. Refer to Alert Sub-Types for more information.

8 Click **Next**.

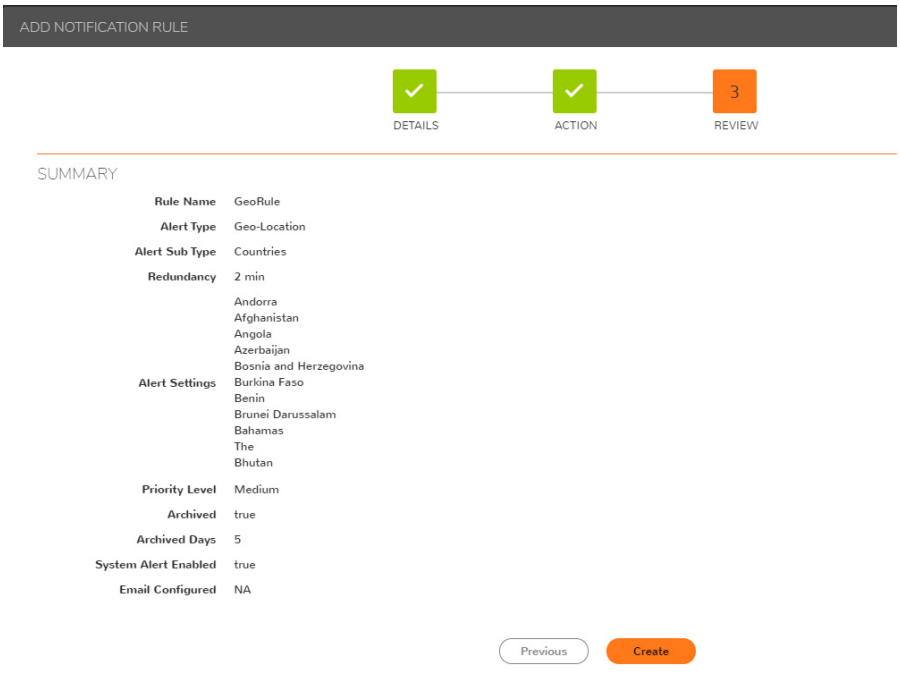


9 Enable **System Alerts,** if needed.

10 Enable **Email** notification and provide the **Email Addresses** of those who should receive the email.

11 Enable **History** by clicking on **Save Notifications** and input the limit for number of days archived.

12 Click **Next**.



13 Validate the definition of your new rule.

14 Click **Create** to save the settings or click **Previous** to make adjustments.

15 Click **Close** and validate that your rule appears in the **Rules** table.

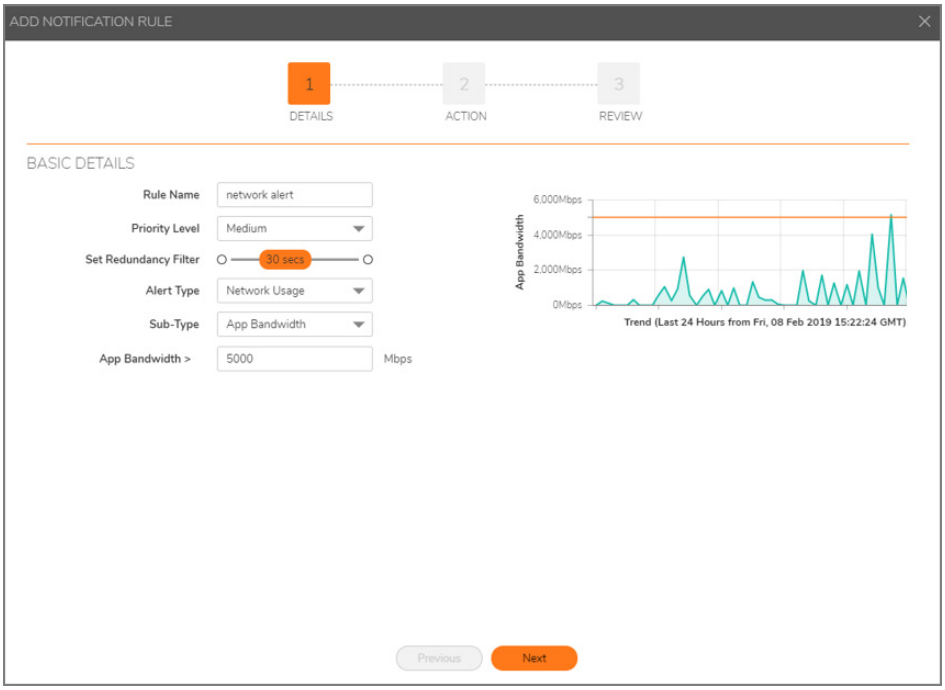
Editing an Alert Rule

Editing an alert rule is very much like adding an alert rule. You are guided through the same process; just changes the fields you want to update.

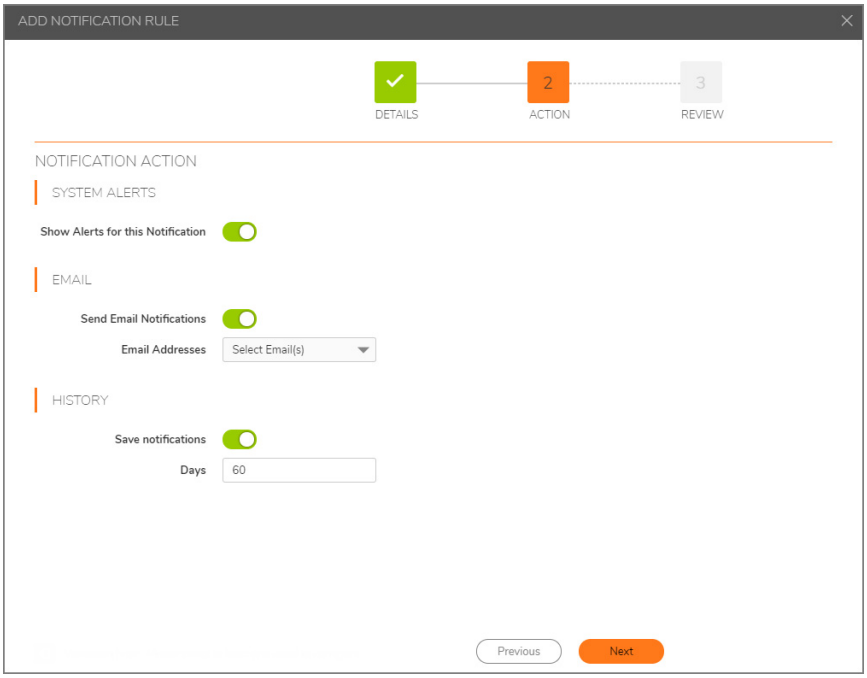
To edit an alert rule:

1 Under the **CONFIGURE** column, click the **Edit** icon.

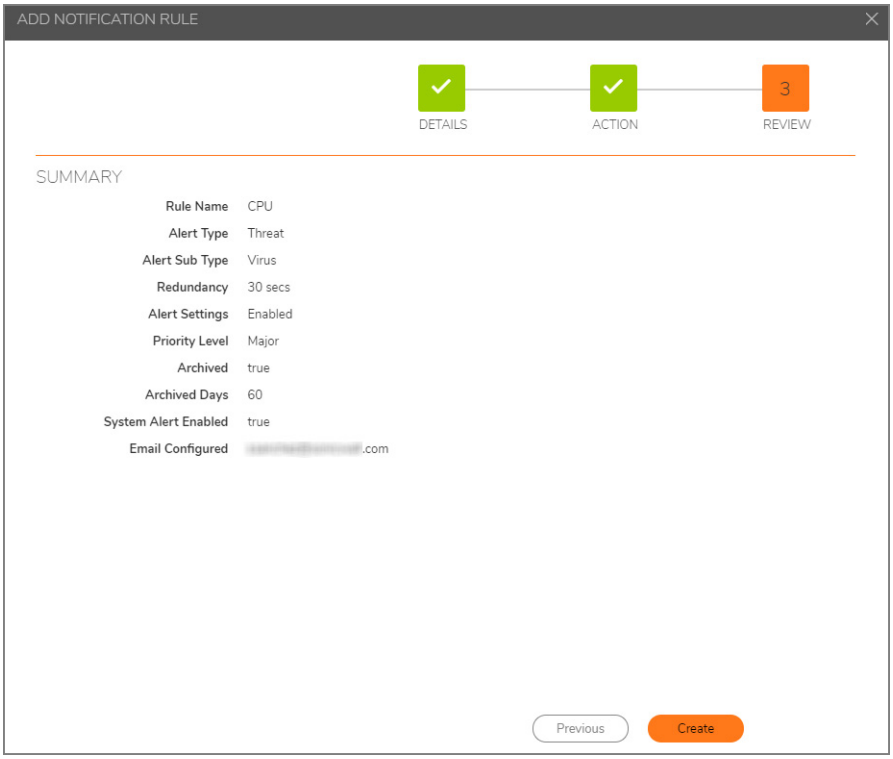
The **ADD NOTIFICATION RULE** dialog window appears allowing you to modify the settings for of the alert.



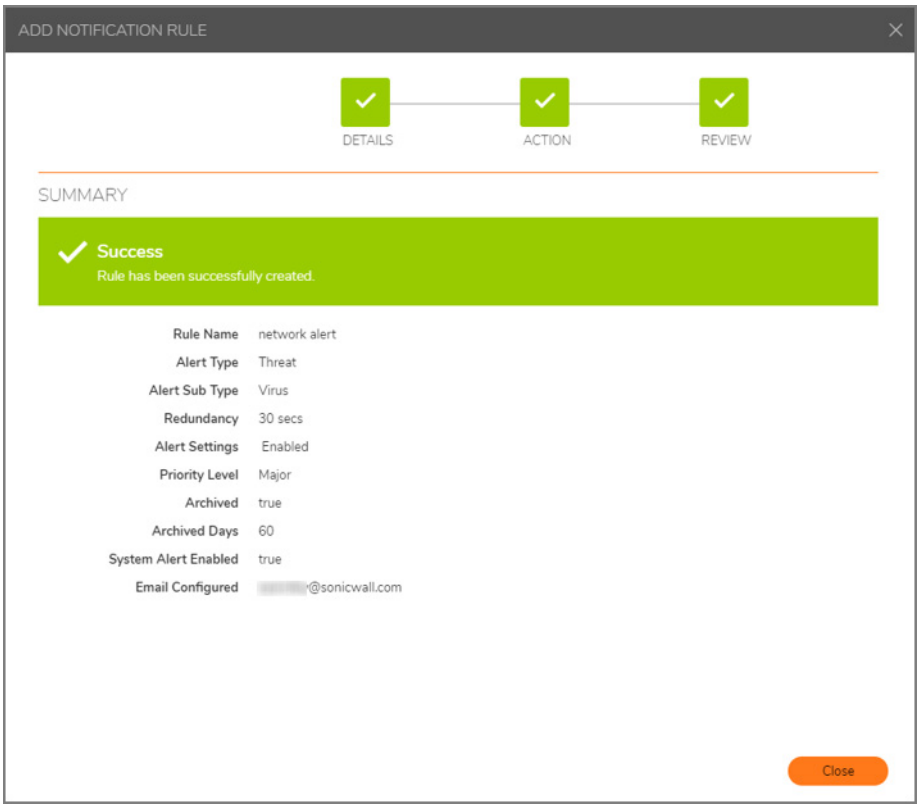
2 On the **DETAILS** page, make any change to the **Basic Details** that are needed and click **Next**.



3 On the **ACTION** screen, update any actions as needed and click **Next**.



4 On the **REVIEW** screen, verify that the **SUMMARY** information is correct and click **Create**.



5 Click **Close.**

Alert Sub-Types

For most of the alert sub-types you have to enter a value on the Details page of the **ADD NOTIFICATION RULE** process. However, you have to take some extra steps with your alert sub-types when you select alert type **Web Activities** or **Geo-Location**.

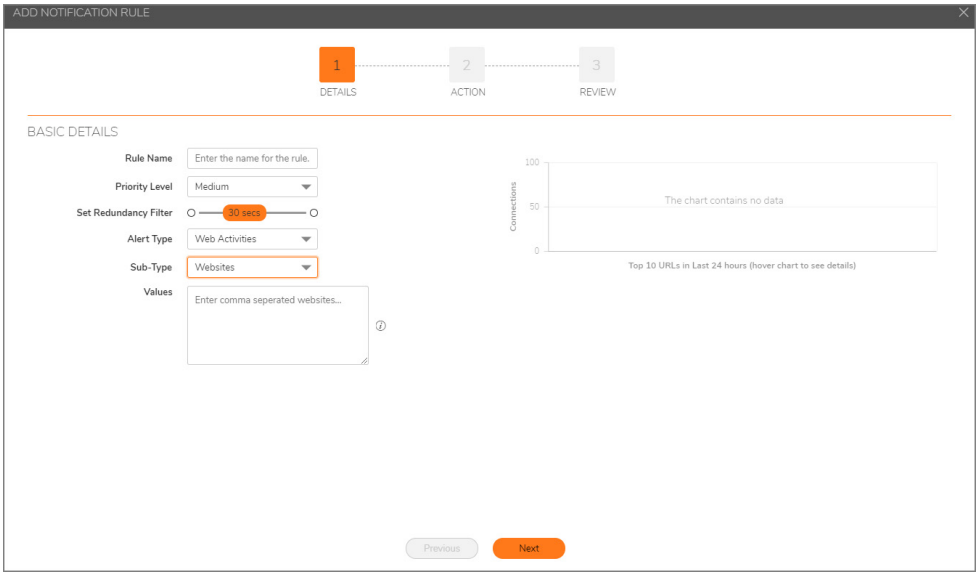
Topics:

Setting an Alert Sub-Type for Web Activities

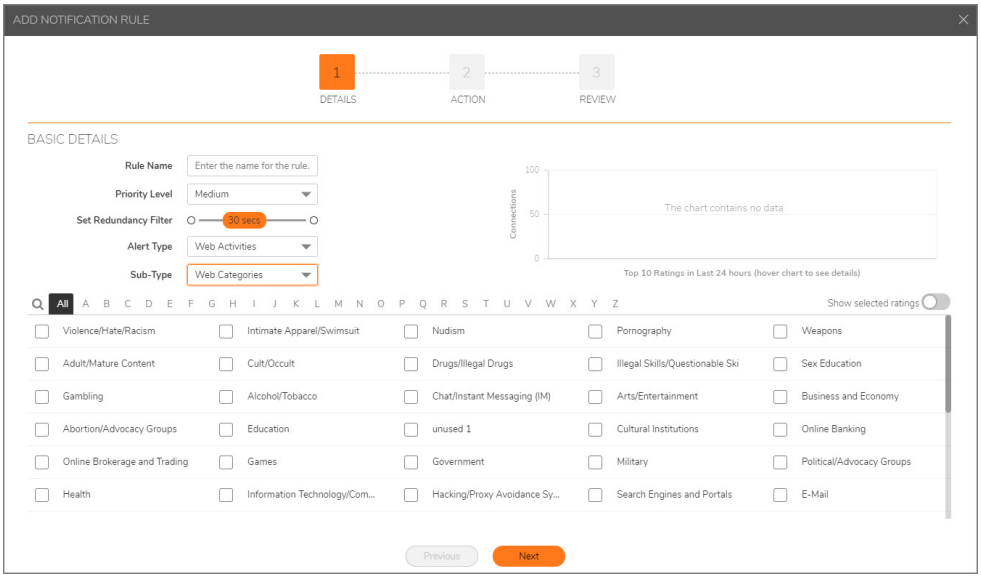
1 Click the **+ Add Alert Rule** icon to add your **Web Activities** alert.

2 Choose either **Websites** or **Web Categories** from the drop-down menu as your Web Activities alert sub-types.

3 If you choose Websites you can enter several websites, or domain names, separated by a comma, in the **Values** text box.



4 If you choose **Web Categories**, you can select several topics by clicking on the check boxes next to the subjects you want.



5 Toggle **Show selected ratings** to get a top-10 rating overview of your web categories in the last 24 hours. The rating is displayed on the graph to the right of the **BASIC DETAILS** dialog window.

> **NOTE:** Hover over the chart to see the ratings detail.

6 Choose the topics for your Web Categories by clicking on the capital letters of the alphabet shown next to the search icon above the subjects.

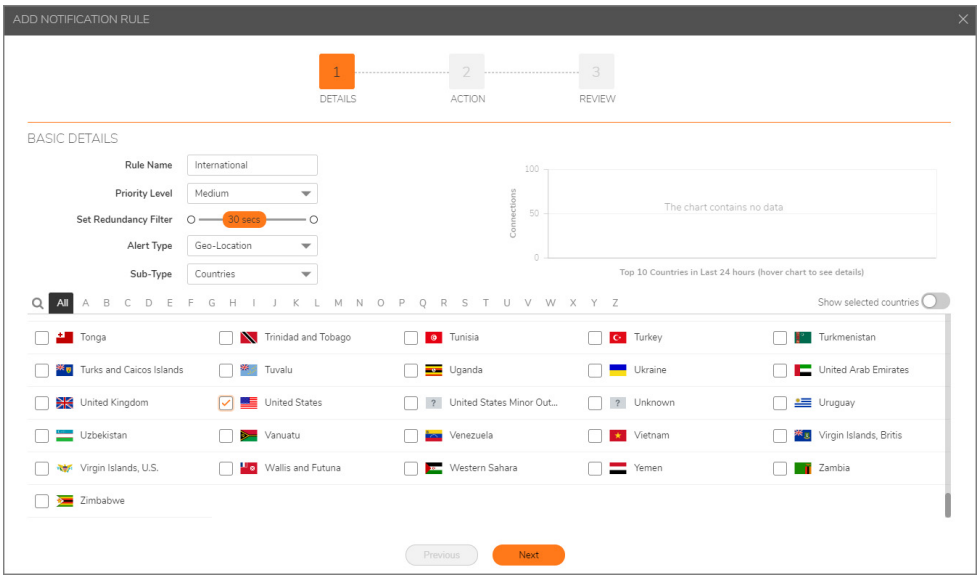
> **NOTE:** The topic for your Web Category is displayed in the **SUMMARY** details of your alert under **Alert Settings**.

7 Click **Create** and then click **Close**.

Setting an Alert Sub-Type for Geo-Location

1 Click the **+ Add Alert Rule** icon to add your **Geo-Location** alert.

2 Choose **Countries** from the drop-down menu as your Geo-Location alert sub-type.



3 Toggle **Show selected ratings** to get a top-10 rating overview of your countries category in the last 24 hours. The rating is displayed on the graph to the right of the **BASIC DETAILS** dialog window.

NOTE: Hover over the chart to see the ratings detail.

4 You can also choose countries for your Countries alert sub-type by clicking on the capital letters of the alphabet shown next to the search icon above the subjects.

NOTE: The country for your Geo-Location category is displayed in the **SUMMARY** details of your alert under **Alert Settings**.

5 Click **Create** and then click **Close**.

Deleting an Alert

To delete an alert:

1 Click the check box for the alert you want to delete.

1 Click the **Delete** icon in the **Configure** column.

2 Confirm your selection.

3 Click **OK**.

4

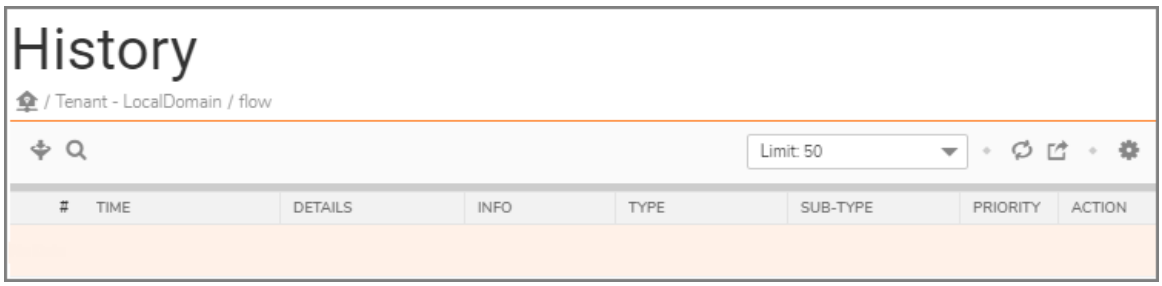
History

The **History** shows the history of the alerts and notifications you received, which is useful for analyzing threats. By saving the data you add an extra layer of protection to your network. The History logs give you the ability to access this data at any time for analysis.

Topics:

History Overview

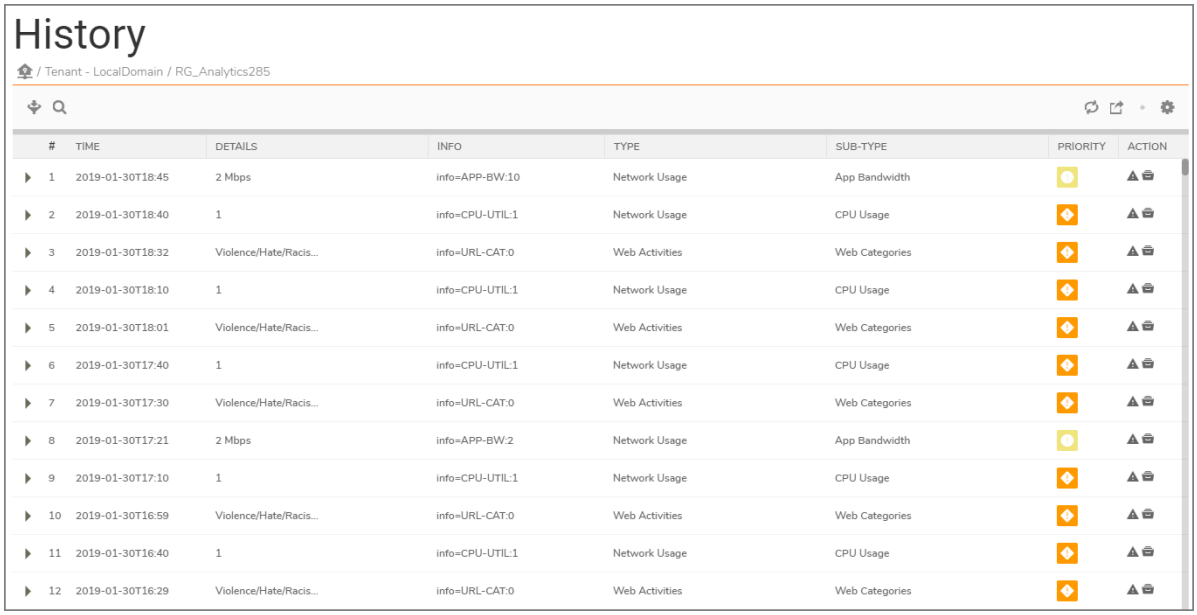
When you enable the History command when you set up a rule, you allow access to folders containing the entire contents of every email created in the logs directory of each server. The logs also analyze email traffic.



Options	Description
Tenant	Allows you to view the tenant or domain for your network that includes your firewall name.
Filter	Allows you to sort by history log priority, type, and sub-type.
Search	Allows you to enter search text to find your history log.
Refresh	Allows you to update the data in the history logs.
Export	Allows you to export/download the data directly from grid view to CSV file.
Show/Hide	Allows you to show or hide the Rules table columns.
Number	The given number of your history logs.
TIME	The time stamp in military standard for your history logs.
DETAILS	The details of each history log.

Options	Description
INFO	The URL, application, CPU, and other details of your alerts based on their type and sub-type.
TYPE	The particular kind or group of your alert.
SUB-TYPE	The sub-type of your broader alert.
PRIORITY	The precedence or rating you give to your alert.
ACTION	The thing you want to do with your alert.

You can click on the caret next to each log item to get details about it. Your **History** table can display hundreds of logs giving you particular information about the time, characteristics, and in what alarm type and sub-type they fall under.



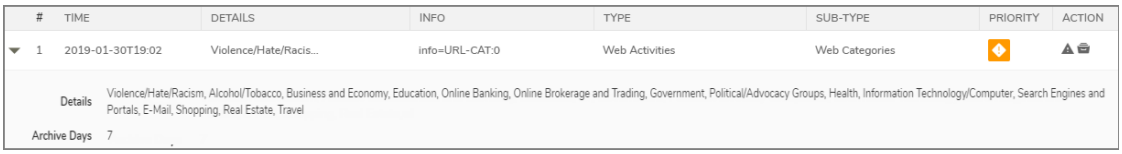
Reviewing History Log Details

To review the details of a log entry:

1 Click the history log you want details for.

2 Click the side caret key to expand an alert and see the details.

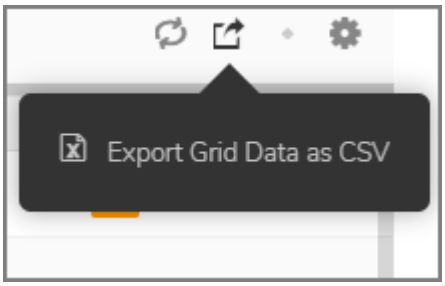
NOTE: The details of your history log also give you the number of days you have archived it for.



Exporting Grid Data as a CSV File

To export the History table:

1 Click the export icon at the top right corner of the History table to get your report.



2 Click on your downloaded Excel document to open it.

NOTE: Your CSV log file includes alert names, types, and sub-types.

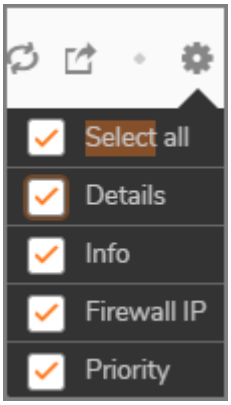
Customizing History Table Columns

Some fields in the History table can be customized to show or hide. The **Details**, **Info**, **Firewall IP**, and **Priority** columns have that option.

1 Click the **Select Columns to Show/Hide** icon.

2 Click the check box next to the column you want to show or hide.

3 Click Select All to show all table columns.



Filtering Your History Logs

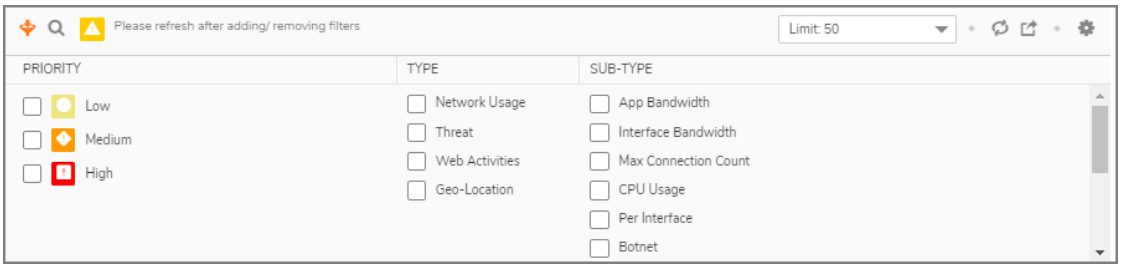
You can filter your history logs by using the filter icon in the top left corner of the History table.

1 Click the **Filter** icon.

2 Choose the limit for your history logs. You can set a limit of 50 (default), 100, 250, 500, 1,000, or 800 (max).

3 Select the options you want to filter on. You can choose options under **PRIORITY**, **TYPE**, or **SUB-TYPE**.

4 Click the filter icon again to return to your normal view of the table.



5

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

SonicWall Firewall Management NOTIFICATIONS Administration
Updated - October 2019
232-005150-00 Rev A