SonicWall® SonicOS 6.5 About SonicOS

Administration

SONICWALL®

Contents

- How to View Legal Information on page 7

About Configuring and Managing the System

For information about configuring and managing the system	See
MANAGE: **System Setup**: • **Appliance**: Base settings, SNMP, passwords, login security, web management, certificates, and system time and schedules • **Users**: User authentication, local users and groups, guest services and accounts, web login, RADIUS accounting, customized pre- and post-login banners, acceptable use policies, and login pages, partitions (adding authentication partitions and partition selection policies) • **Network**: Interfaces, PortShield interfaces and X-Series switches, failover and load balancing, zones, VLAN translation, DNS, DNS proxy, routing, ARP, neighbor discovery, MAC-IP anti-spoof, DHCP server, IP helper, web proxy, and dynamic DNS • **SD-WAN**: SD-WAN groups, performance probes, performance class objects, path selection profiles, SD-WAN route policies, SD-WAN monitor, and SD-WAN connections logs • **Switching**: VLAN trunking, L2 discovery, link aggregation, port mirroring • **High Availability** (HA): base setup and advanced and monitoring settings • **WAN Acceleraton**: Enables and configures WAN Acceleraton on WXA series appliances • **VOIP**: Consistent NAT and SIP and H.323 settings • **Virtual Assist**: Configures access to your security appliance by clients for assistance and technical support	*SonicOS 6.5 System Setup*
QUICK CONFIGURATION: An initial system setup with quick configuration guides (wizards): • **Setup Guide**: Configure basic settings for the SonicWall security appliance to secure your internet connection • **Public Server Guide**: Provide public access to an internal server • **VPN Guide**: Create site-to-site VPN policies or configure the WAN GroupVPN to accept connections from the Global VPN client • **App Rule Guide**: Configure security features for App rule • **WXA Setup Guide**: Configure a coupled WXA series appliance for WAN acceleration	*SonicOS Quick Configuration*
Connectivity: • **VPN**: Base settings, advanced settings, DHCP over VPN,L2TP server, AWS VPN • **SSL VPN**: Server settings, client settings, portal settings, Virtual Office • **Access Points** (SonicPoint/SonicWave): Dashboard, base settings, floor plan view, topology view, IDS, advanced IDP, packet capture, virtual access point, FairNet, Wi-Fi multimedia, 3G/4G/LTE WWAN • **3G/4G/Modem**: Base settings	*SonicOS 6.5 Connectivity*

For information about configuring and managing the system	See
Policies: • **Rules**: Access rules, app rules and control, NAT policies • **Objects**: Address, match, action, service, email address, content filter, AWS, dynamic external, and bandwidth	*SonicOS 6.5 Policies*
Updates: • **Licenses**: provides links to activate, upgrade, or renew SonicWall Security Services licenses and allows you to manage all the licenses for your SonicWall security appliance • **Firmware &Backups**: provides settings that allow for easy firmware upgrade and preferences management. • **WXA Firmware**: provides options to check for upgrades, perform a factory reset, and automatically download a WAN Acceleraton firmware upgrade for your WXA series appliance • **Restart**: restarts the SonicWall security appliance	*SonicOS 6.5 Updates*
Security: • **Firewall settings**: advanced security appliance settings (detection protection, connections with DPI, Access rule options jumbo frames, IPv6 configuration, control plane flood protection) bandwidth management (BWM), flood protection, multicast, QoS mapping, and SSL control • **Security services**: base settings, content filtering (CFS) settings, client AV and CF enforcement, Gateway anti-virus, intrusion prevention, capture ATP, anti-spyware, and RBL, GEO-IP, and Botnet filters • **Decryption services**: Deep Packet Inspection (DPI) (DPI-SSL/TLS client and server; DPI-SSH) • **Anti-spam**: basic and advanced settings, real-time blacklist filter, relay domains, junk box settings and summary, user view setup, address books, manage user, LDAP configuration, anti-Spam tools	*SonicOS 6.5 Security Configuration*
Logs & Reporting: • **AppFlow settings**: use to configure, manage, and monitor AppFlow and real-time data sent a local collector or external AppFlow servers in external AppFlow reporting formats, such as NetFlow version 5, NetFlow version 9, IPFIX, and IPFIX with Extension • **Log settings**: use to categorize and customize the logging functions on your SonicWall security appliance for troubleshooting and diagnostics	*SonicOS 6.5 Logs and Reporting*
Legal information: • Access the SonicWall End User Product Agreement (EUPA) as well as other legal information	How to View Legal Information on page 7
API: • Display the SonicWall SonicOS API Agreement, which contains a link to SonicOS API online documentation, as well as other legal information	About the API/CLI on page 8

About Monitoring the System

For information about monitoring the system	See
MONITOR:	*SonicOS 6.5 Monitor*
Dashboard: Summarizes much of the data from the AppFlow report, while highlighting key data from the latest report	
Event summaries: • **Threat protection**: displays real-time threat protection data from SonicWall security appliances deployed around the world • **Capture ATP**: provide information for each file that it has scanned for viruses and malware • **Spam Statistics**: displays the statistics for the SonicWall Anti-Spam service, including total connections blocked due to spam, phishing, or viruses	
Appliance Health: • **Overview**: displays reports showing the security appliance's top applications, users, IP addresses, viruses, intrusions, spyware, URL ratings, locations, and IP addresses • **Live Monitor**: provides a real-time, multi-functional display with information about hardware multi-core utilization, applications, bandwidth usage, packet rate, packet size, connection rate, connection count, and memory usage • **Bandwidth Monitor**: displays policy-based bandwidth usage for ingress and egress network traffic, and a second chart with the top 10 for policy-based bandwidth usage • **Protocol Monitor**: displays real-time charts showing ingress and egress traffic rates for the IPv4, ARP, IPv6, UDP, TCP, ICMP, and IGMP protocols • **SD-WAN Monitor**: displays real-time charts showing latency, jitter, and packet loss	
Current status: • **System Status**: provides system information such as firmware version and system up time, security services license status, the latest alert messages, and network interface zone assignments, IP addresses, and link status • **User Sessions**: displays current information about various types of users connected to the network security appliance, including SSL VPN users, active users, and guest users • **High Availability Status**: displays the current status of the High Availability pair, including state of primary and secondary units, mode and link configuration, and licenses • **High Availability Status**: displays the current status of the High Availability pair, including state of primary and secondary units, mode and link configuration, and licenses • **Anti-Spam Status**: displays the state of your Anti-Spam Service license and the status of your servers. You can also capture and perform diagnostics on an email stream, look up MX records, and do GRID IP checks on host IP addresses	

For information about monitoring the system	See
• **Access Point Stations**: displays the statistics of each SonicWall SonicWave and SonicPoint wireless access point connected to the SonicWall security appliance, along with statistics and information for all connected client stations	

About Investigating Problems

For information about investigating problems	See
INVESTIGATE: • **Logs**: Event, connection, Appflow, WAN Acceleration, Anti-Spam Junkbox, SD-WAN Connection Logs • **Reports**: Appflow, RF Analysis, TCP and WFS acceleration, WXA web cache • **Tools**: Packet monitor, Packet replay, network probes, system diagnostics	*SonicOS 6.5 Investigate*

How to View Legal Information

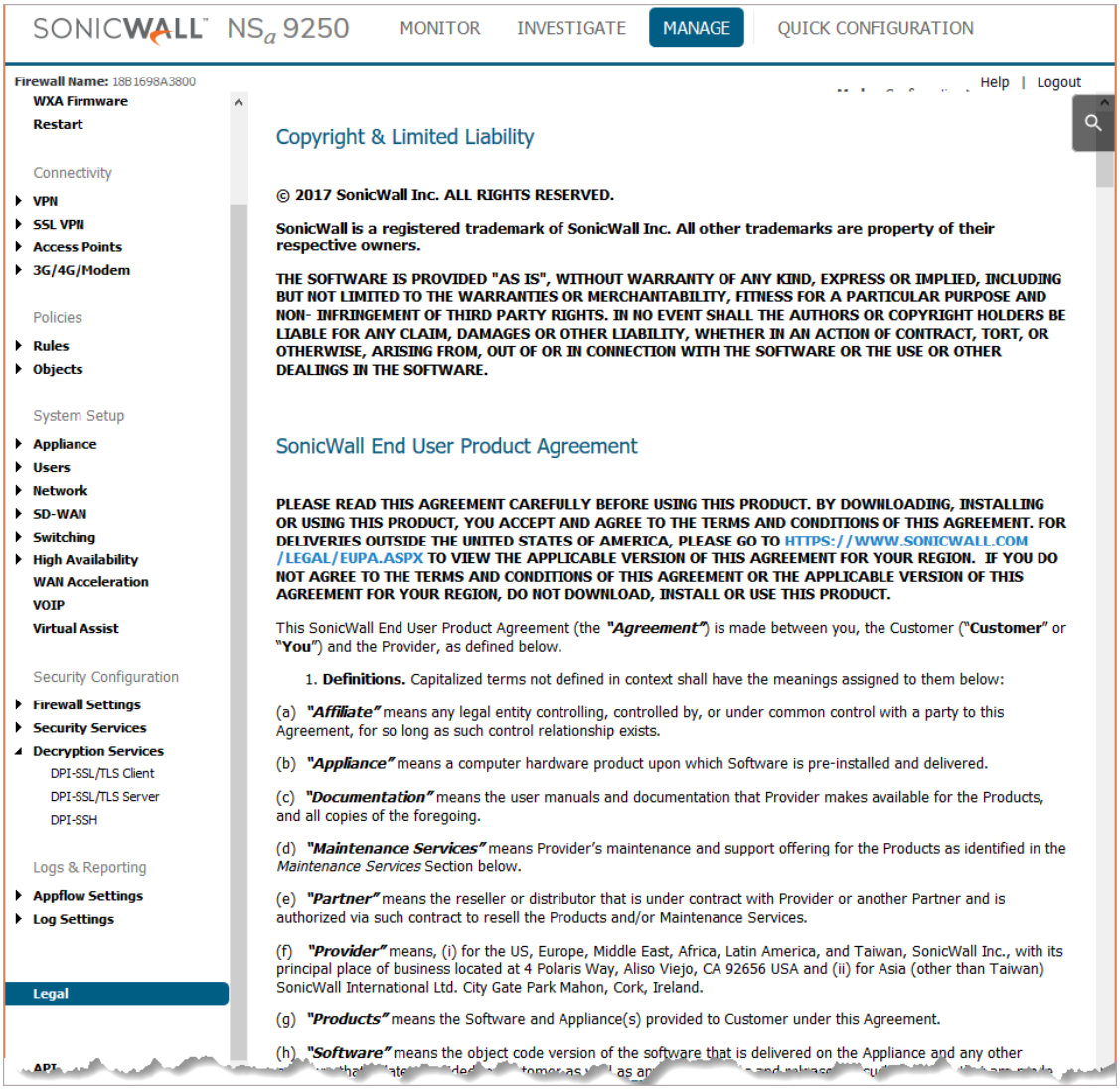
You can access the copyright, limited liability, and SonicWall End User Product Agreement (EUPA) easily from the management interface.

To view legal information:

1 Navigate to the **MANAGE** view.

2 Scroll to the bottom of the navigation pane.

3 Click **Legal**. The **Legal** page displays.



About the API/CLI

The SonicOS Enterprise Command Line Interface (E-CLI) provides a concise and powerful way to configure SonicWall security appliances without using the SonicOS web-based System Setup. You can use the CLI commands individually on the command line or in scripts for automating configuration tasks.

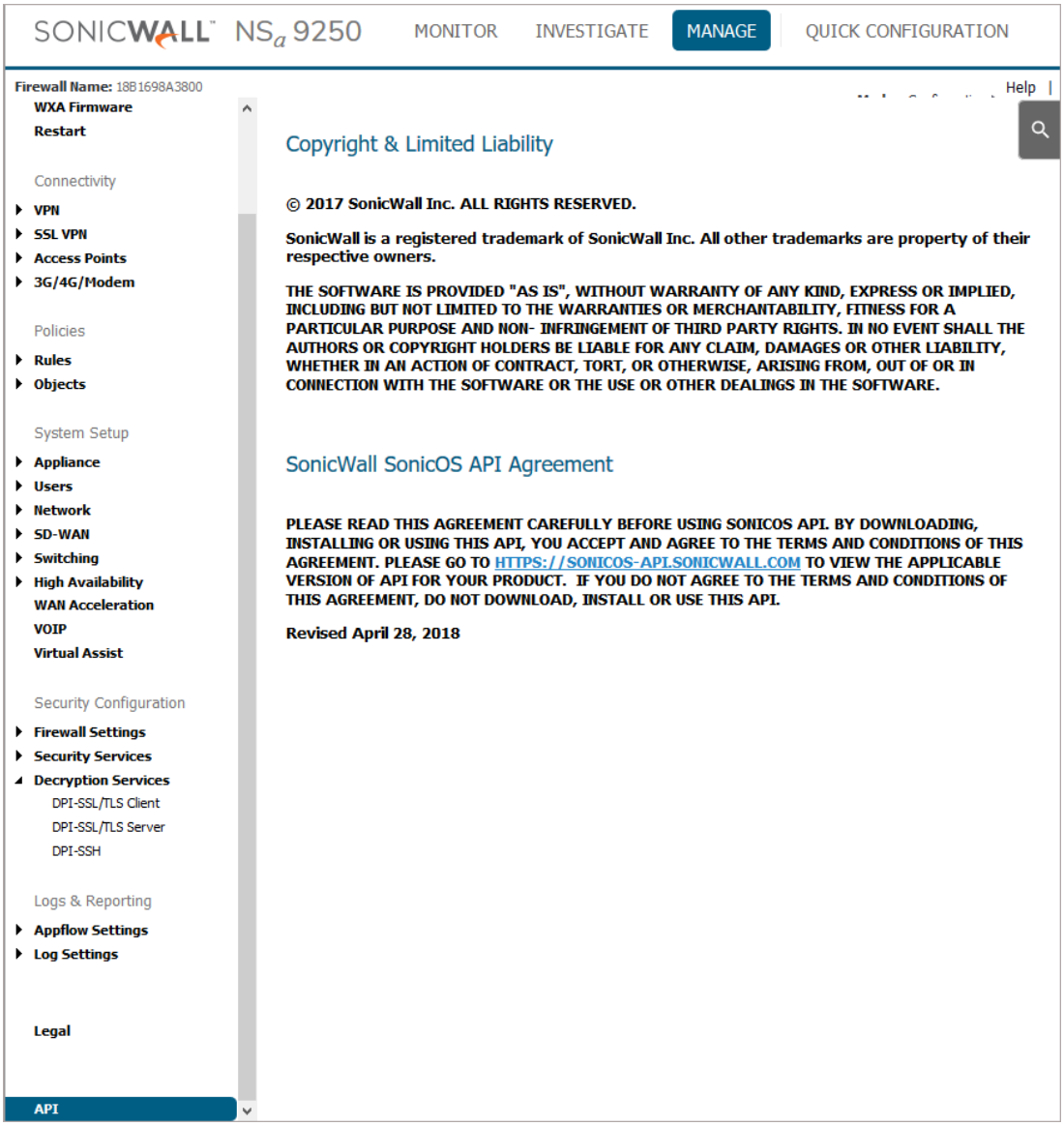
SonicOS's API (Application Program Interface) provides an alternative method to the SonicOS CLI for configuring selected functions.

To view SonicOS API:

1 Navigate to the **MANAGE** view.

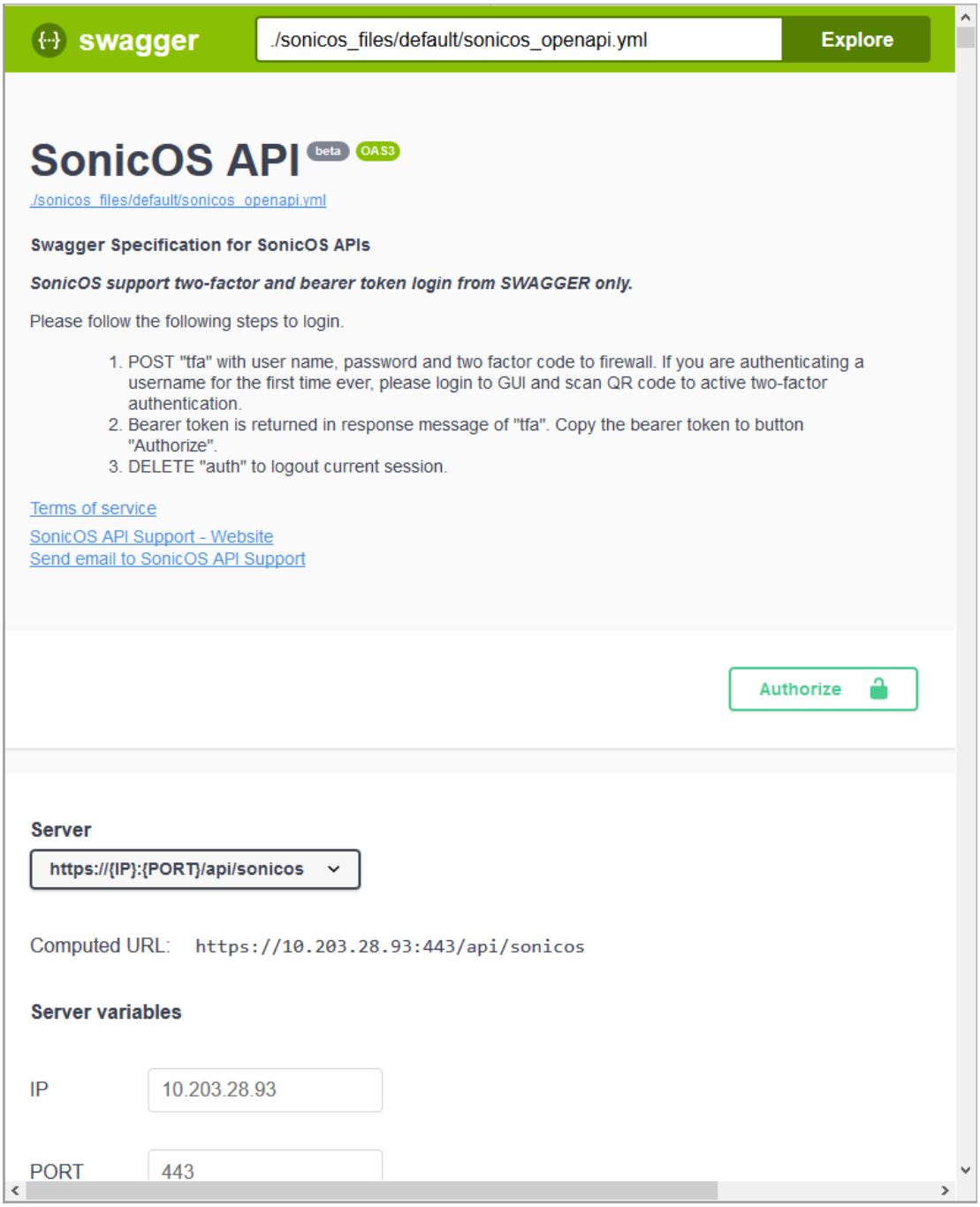
2 Scroll to the bottom of the navigation pane.

3 Click **API**. The **API** page displays.



4 Scroll to **SonicWall SonicOS API Agreement**.

5 Click the link, **HTTPS://SONICOS-API.SONICWALL.COM**. The Swagger page for SonicOS API displays.



Task-Oriented Management Interface

The SonicOS management interface is designed for user experience and ease of use. Based on usability studies, the management interface is organized into high-level tasks, with the top-level task in a menu in the header:

Monitor	Dashboards and graphs provide overall status of device and traffic statistics along with a threat prevention summary for overall traffic that is traversing the security appliance.
Investigate	Logs, reports, and some investigative tools, such as packet monitor, to identify a network or security incident and its remedy.
Manage	Setup and configuration for the entire security appliance; used during initial setup, renewals, upgrades, and facilitates applying any remedies discovered during an investigation.
Quick Configuration	Guides (wizards) for quickly setting up and configuring a basic SonicOS system.

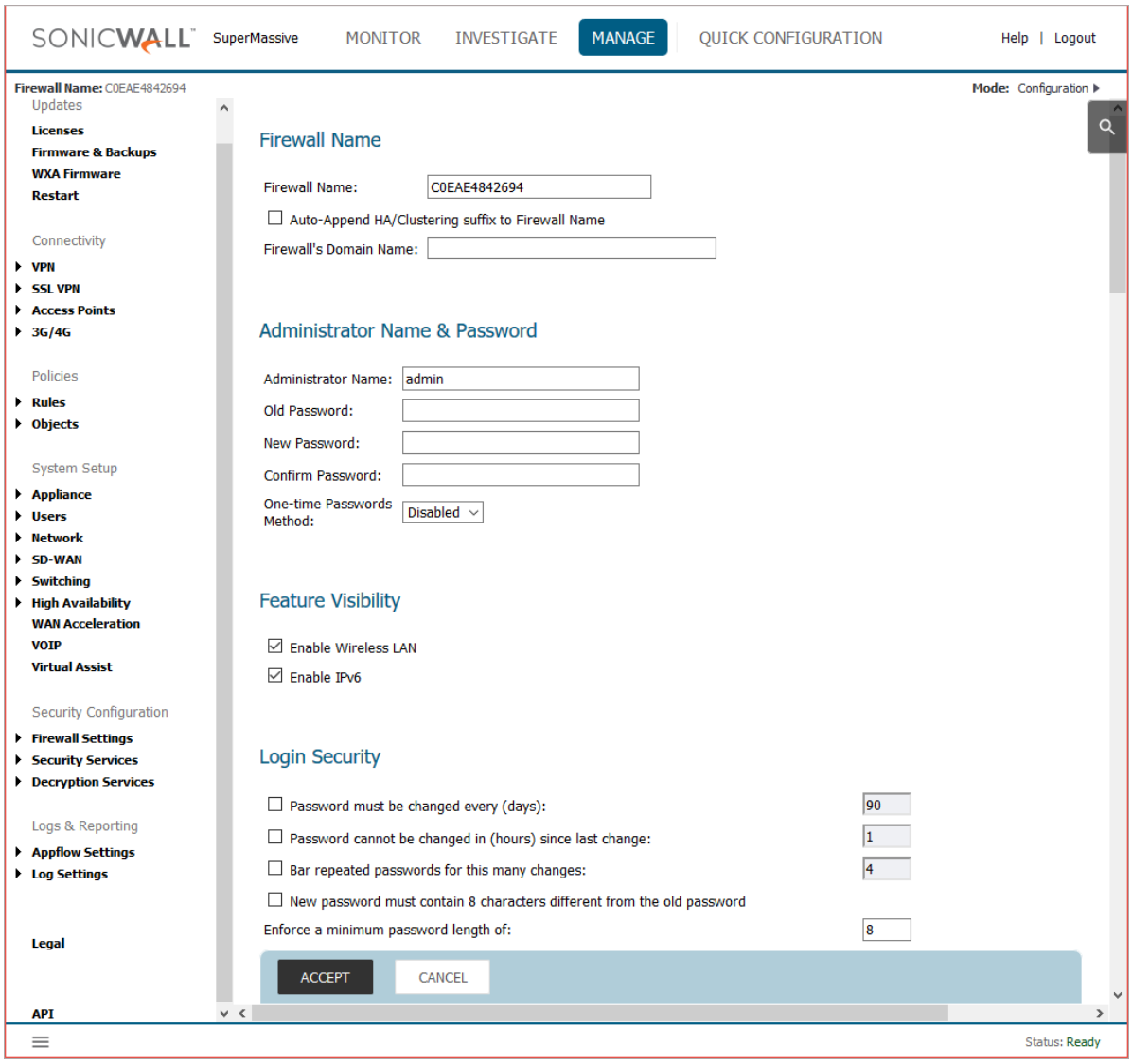
For further information about the SonicOS management interface, see SonicOS Management Interface on page 14.

Topics:

Task-Oriented Navigation

Clicking an entry in the top-level task menu displays a task-oriented, left-hand navigation menu. The items in the navigation menu have been reorganized and grouped under labels for easier navigation, and some have been

renamed. This functional breakdown makes it easier to complete tasks without switching between the top-level sections, and to determine the correct section at the start of each new task.



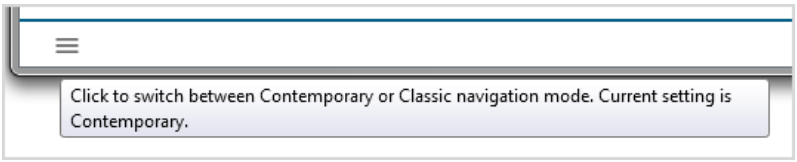
Dashboards

The default **Dashboard** page summarizes much of the data from the Capture Threat Assessment report. This dashboard provides the “here’s what's going on, and here’s what was blocked” information you need. In addition, the top of the dashboard provides general system and network health information to support your investigation tasks. Finally, the dashboard brings the wealth of security services and features available in the security appliance to the forefront.

The large majority of the data relies on Real-time Data Collection and Aggregate AppFlow Report Data Collection being enabled. If one or both of these functions is not enabled, the dashboard presents some empty states.

Using the Classic Navigation Style

SonicOS still supports the classic SonicOS navigation of previous versions. To toggle between the contemporary and classic navigation styles, click the **Navigation** icon at the bottom of the left navigation pane.



2

SonicOS Management Interface

About the SonicOS Management Interface

To help you configure, manage, monitor, and solve problems, the SonicOS management interface comprises three views and a set of quick configuration guides:

- **MANAGE** view; see About the MANAGE View on page 14
- **QUICK CONFIGURATION** guides; see About the Quick Configuration Guides on page 15
- **MONITOR** view; see About the MONITOR View on page 16
- **INVESTIGATE** view: see About the INVESTIGATE View on page 16

You select the view or **QUICK CONFIGURATION** by clicking in the SonicOS banner:

About the MANAGE View

The **MANAGE** view in the web-based, graphical management interface provides a convenient way to configure and manage your SonicWall network security appliance(s) running SonicOS 6.5 and higher. Using the **MANAGE** view, you can:

Configure the SonicWall security appliance to meet your security needs	• Set up your network environment, including servers, SonicPoints, SonicWaves, WXA series appliances, Dell X-Series switches and N-Series switches • Create interfaces, zones, and routing • Create policies, rules, and objects to refine control of incoming and outgoing traffic • Create SD-WAN groups, performance probes, path-selection profiles • Create VPN policies to support Global VPN clients and connecting SonicWall security appliances in remote offices • Configure SSL VPN settings to provide secure, seamless, remote access to resources on your local network • Configure high availability systems, failover, and load balancing • Add security services such as anti-spam, anti-phishing, and anti-virus capabilities • Add decryption services such as DPI-SSL/TLS and DPI-SSH • Authenticate and managing users, groups, and guests • Manage bandwidth • Filter traffic with black lists and white lists as well as RBL, GEO-IP, and Botnet filters • Provide online customer technical support
Configure logs and logging	Configure App Visualization, Analyzer, and logs, such as SYSLOG and AWS, to your requirements
Access legal information	Display the copyright, limited liability agreement, and SonicWall End User Product Agreement (EUPA)
API	Display the copyright, limited liability agreement, and SonicWall SonicOS API Agreement, which contains a link to SonicOS API online documentation.

About the Quick Configuration Guides

The Quick Configuration guides are a set of wizards that provide step-by-step instructions for quickly setting up a basic system that you can then modify:

This guide	Steps you through
Setup Guide	Network configuration for Internet connectivity **NOTE:** The TZ series and SOHO series security appliances have an initial Setup Guide that displays when you first start up the security appliance.
PortShield Interface Guide	Selecting the initial ports assignment in integrated managed LAN switch of the SonicWall security appliance
Public Server Guide	Adding a server to your network, such as a mail server or a Web server
VPN Guide	Configuring Group VPNs and site-to-site VPNs
App Rule Guide	Creating an App Rule
WXA Setup Guide	Configuring the coupled WXA series appliance for WAN Acceleration

NOTE: Some guides require the feature to be licensed before being available.

About the MONITOR View

The **MONITOR** view in the SonicOS management interface provides dashboards and graphs designed to help you quickly monitor the health and status of your security appliance and networks.

Using the **MONITOR** view, you can see a summary of what is happening on the SonicWall security appliance and what is passing through it. Effective flow charts of real-time data, Capture ATP results, system status, and SonicWall Threat Reports are displayed for quick analysis. You can:

Monitor the:

- Status of your network
- Appliance health
- User and guest sessions
- Bandwidth and protocols
- Performance probes
- Traffic consumption
- Applications
- Threat prevention
- Packets

View reports by:

- Appflow
- RF analysis
- TCP or WFS acceleration

About the INVESTIGATE View

The **INVESTIGATE** view provides logs, reports, and tools designed to help you quickly notice and respond to potential problems with the health and status of your security appliance and networks. You can:

View real-time data logs:

- Event logs for tracking potential security threats
- Connection logs for tracking all active connections to the SonicWall security appliance
- Appflow logs provide real-time, incoming and outgoing network data
- WAN Acceleration logs lists detailed log event messages and provides multiple options to change how the log messages display
- Anti-Spam Junkbox for viewing, searching, and managing messages currently in the Junk Store on the Exchange or SMTP server
- SD-WAN connection logs

View reports:

- Appflow Reports provides configurable scheduled reports by applications, users, IP addresses, viruses, intrusions, spyware, locations, botnets, and URL rating along with statistics to provide a top-level aggregate report of what is going on in your network
- Log Reports displays a rolling analysis of the top 25:
  - Most frequently accessed Web sites
  - Users of bandwidth by IP address
  - Services consuming the most bandwidth
- RF Analysis displays data to help you best utilize wireless bandwidth with wireless access point appliances
- TCP Acceleration Reports provides statistics and graphs for viewing and monitoring the TCP Acceleration on your WXA series appliance(s)
- WFS Acceleration Reports provides statistics and graphs for viewing and monitoring the WFS Acceleration on your WXA series appliance(s)
- WXA Web Cache Reports provides the statistics for investigating the Web Cache service on your WXA series appliance(s)

Use tools to monitor your system and its traffic:	• Packet Monitor allows you to monitor individual data packets, either monitored or mirrored, that traverse your SonicWall security appliance • Packet Replay for testing and debugging by replaying packets by crafting a packet, using the packet buffer, or replaying a Pcap file • Network Probes provides a flexible mechanism for monitoring and displaying network path viability • System Diagnostic provides diagnostic tools that help troubleshoot various kinds of network problems and process monitors.

About Key Management Interface Features

Topics:

About the Dynamic User Interface

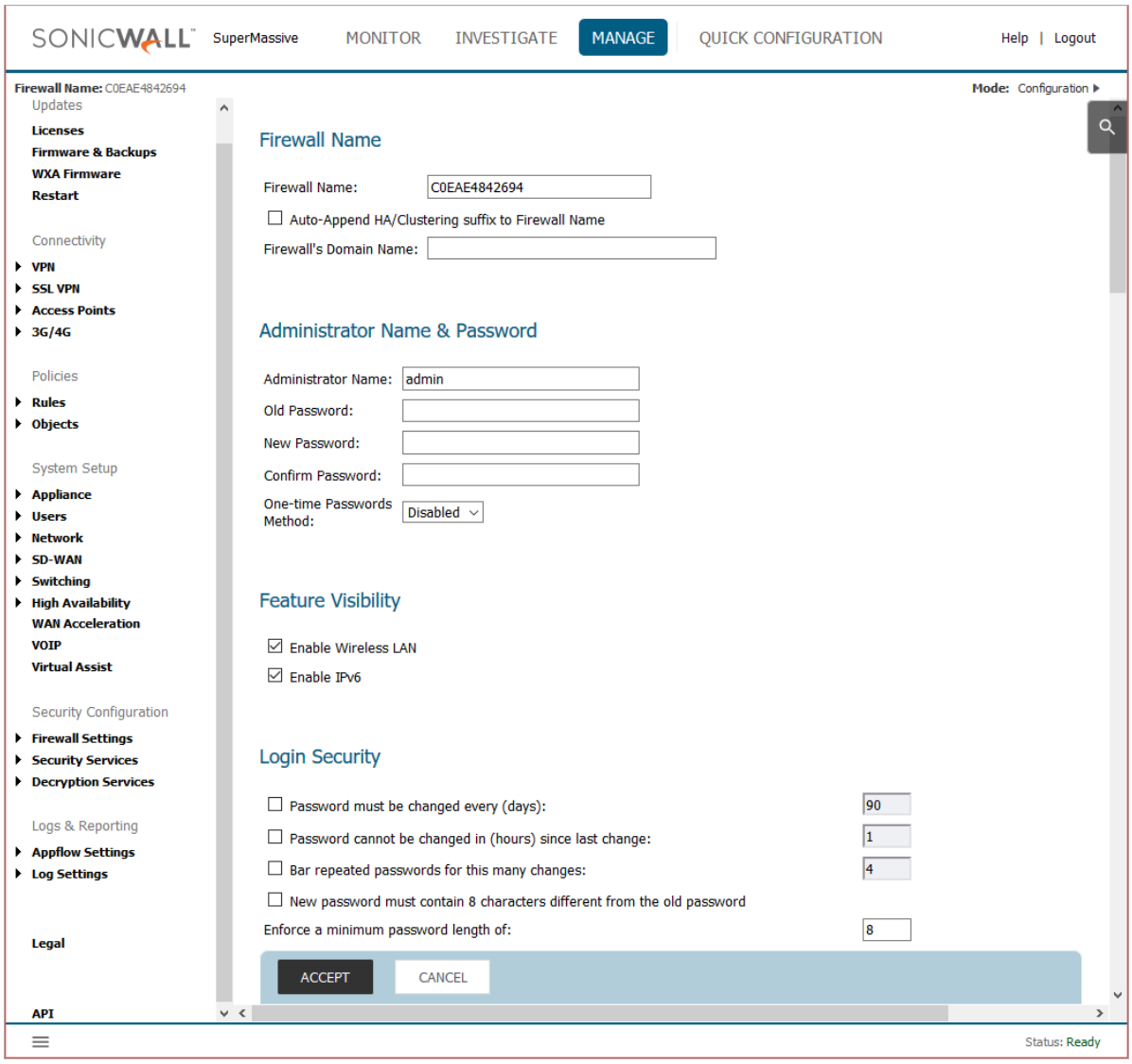
Table statistics and log entries are dynamically updated within the Management Interface without requiring you to reload your browser. Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the **Delete** icon in the **Flush** or **Logout** column.

This dynamic interface is designed to have no impact on the Web server, CPU utilization, bandwidth or other performance factors. You can leave your browser window on a dynamically updating page indefinitely with no impact to the performance of your security appliance.

Navigating the Management Interface

Navigating the management interface is facilitated by a hierarchy of menu items in the navigation pane (left side of your browser window) that are subordinate to the top-level task menu in the header. When you click a menu

item, related management functions are displayed as submenu items in the navigation pane. Some of these pages are further subdivided with a menu across the top of the page.



If the navigation pane continues below the bottom of your browser, use the slider or scroll wheel on your mouse.

Consistency of Management Interface Settings

As you move from management interface page to management interface page, you retain the settings through every login. For networks with multiple administrators, SonicOS provides this ability to each admin user, maintaining the settings for each administrator even when other administrators log in through the same browser. This feature also offers options to store/retrieve client-side data shared across users or pages.

Some common uses for this feature are restoring:

- The last visited page for different logged-in administrators.
- Displaying options of certain table pages. For instance, display options such as IP version, view type and From/To zone in the **MANAGE | Network > Rules > Access Rules** page can be restored for different administrators although only certain table pages can benefit from this feature, such as the **Access Rules** page.

Icons and Buttons in the Management Interface

Topics:

Icons

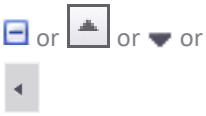
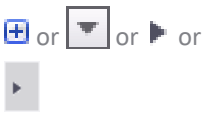
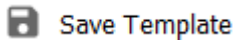
The management interface uses icons to facilitate certain actions. Some icons are common throughout the management interface while others apply to only one or two pages. Icons describes the functions of common icons used in the management interface:

Icons

Action	Icon	Description
ADD/CREATE		

Add/Create		Either:
		• Displays a:
		  • Dialog or menu that allows you to add elements, such as zones, services, and access/firewall rules, to your security appliance.
		  • Dialog (secondary or popup window) for adding entries to a table.
		  • Dialog for creating a firmware backup for your security appliance.
		• Enables a built-in common name.

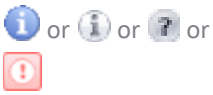
Icons

Action	Icon	Description
CHART FORMATS		
Chart Format:		Toggles the display of a chart between bar and flow (area) formats.
Bar Chart		Displays the bar format of a chart.
Flow (Area) Chart		Displays the flow (area) format of a chart.
CLEAR		
Clear Logs		Clears all logs.
Clear Statistics		Updates the statistics shown in the traffic tables.
Clear Stats		Clears traffic statistics.
COLLAPSE/EXPAND		
Collapse		Hides or shrinks a chart, table, or section of a management interface page to allow more display room for other data.
Expand		Redisplays or expands a hidden chart, table, or section of a management interface page.
CONFIGURE/SETTINGS		
Boot		Reboots the security appliance with the firmware version listed in the same row.
Configure		Allows for customization of the display. The function changes with the page containing the icon. **NOTE:** The **Configure** icon and **Configure** button have different functions.
Cloud		Indicates an action that can be done on the cloud.
Edit		Displays a dialog (secondary page or popup) for editing the settings.
Junk Store Installer		Launches the Junk Store Installer wizard.
Restore		Restores default values to table entries.
Save Template		Displays a popup for saving the log settings to a custom template.
Settings		Displays a popup for configuring options.
DELETE/FLUSH/PURGE		
Delete		Deletes a table entry. Some system-generated entries cannot be deleted, and their icons are dimmed and modified ( ).
		Indicates a drop-down menu for selecting whether to delete the selected table entries or all table entries.
Flush		Clears the downloaded IPs of Botnet servers.

Icons

Action	Icon	Description
Purge	Purge	Displays a drop-down menu for selecting which objects to delete from a table: • **Purge** (selected objects) • **Purge All**
DISPLAY		
Display		Opens a new tab in your browser that displays only the report or graph associated with a submenu item. For more information, see Display Icon on page 24.
Display Appflow Reports Page		Displays the **INVESTIGATE | REPORTS | Appflow Reports** page.
Display Options		Displays a menu or popup with options that control how data are displayed in the table.
Go To		Go to the specified entry in the table.
IPv4/IPv6		Displays both IPv4 and IPv6 entries in a table.
		Displays and indicates IPv4 entries in a table.
		Displays and indicates IPv6 entries in a table.
Matrix View		Displays a matrix dialog for choosing zones.
View		Indicates the local view.
Navigation		Toggles between the Contemporary view of the management interface and the Classic view.
DOWNLOAD/EXPORT/IMPORT/PRINT/UPLOAD		
Download	Download	Downloads the IPs of Botnet servers from the configured server.
Export		Exports: • Firmware configuration. • VPN policy to a file in either encrypted or non-encrypted format.
		Exports the data flow into a comma separated variable (.csv) file. The default file name is **sonicflow.csv.**
		Displays a drop-down menu for selecting the type of file for exporting: • CSV-format (`.csv`) file • Plain text-format (`.txt`) file • Email
Import		Imports configuration or certificate information or images.
Download		Downloads and reboots the security appliance with the firmware version listed in the same row.
Import Template	Import Template	Displays a popup dialog for selecting and downloading a log category template.
Print		Exports the data flow to a printer or file.
Print PDF Report		For some UI pages, prints a pdf file.

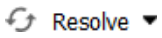
Icons

Action	Icon	Description
Upload		Uploads a file to a common database or external switch.
		Displays a dialog for uploading a signed certificate.
ENABLE/DISABLE		
Enable Cloud Backup		Enables cloud backup.
Enable/Disable LLDP		Toggles between enabling/disabling LLDP.
FILTERING		
Filter		Displays a filter dialog for refining the data to show only desired entries in the table.
Delete Filter		Deletes a saved filter.
Load Filter		Loads a saved filter into the filter view.
INFORMATION		
Alert		Indicates when a new firmware release is available.S
Caution		Indicates information about the effects of an action.
Comment		Displays text from a field entry or information about the table entry.
Help		Displays the relevant online help from a global search result.
Information		Displays a popup containing more detailed information than displayed on the page.
		Indicates information about the page, option, or security appliance; may display a popup when moused over.
Search		Searches a table for the specified data. **NOTE:** The **Search** icon and the **Search** button have different functions.
Tooltip		Displays a popup containing information about an option or setting on a page, report, or dialog.
Warning		Indicates information about the effects of an action.
STATISTICS		
Notes		Displays a popup containing status or statistics about an entry in tables.
Statistics		Displays a popup balloon containing statistics about an entry in tables or general status about the table or page.
STATUS		
Blocked		Indicates the cipher has been blocked.

Icons

Action	Icon	Description
Disabled		Indicates the interface or service is disabled or offline. Clicking on the icon enables the interface or service.
		Indicates the option or event is disabled. Clicking on the icon enables the option or event.
		
		Indicates that all members of the category, group, or event are disabled.
Enabled		Indicates: • The interface or service is enabled. Clicking on the icon disables the interface or service. • Logging is enable. Clicking on the icon displays a popup that lists the latest log entries.
		Indicates the option or event is enabled. Clicking on the icon disables the option or event.
		Indicates a service, such as Guest Services, is enabled for the user/group. Mousing over the icon displays a popup message.
		Indicates the firmware version running the SonicWall security appliance.
		Indicates the security services is licensed and enabled.
		Indicates the network interface link is up.
		Solid indicates that all members of the category, group, or event are enabled.
		Semi-solid indicates that some are enabled, some are disabled.
Online		Indicates the access point is operational or disabled.
Offline		Indicates the access point is non-responsive or initializing.
Busy		Indicates the access point is synchronizing/provisioning or scanning.
Status		Indicates the status of the feature: • Green signifies that the feature is active and operating. • Yellow signifies the feature is not active or operating. • Red signifies the feature is disabled.
		
		
UPDATING DATA/TABLES		
Priority		Displays a pop-up for changing the priority of an entry in a table.
Move List Entries		Moves a selected list entry up or down in the list.

Icons

Action	Icon	Description
Pause		Freezes the data flow. The time and date also freeze. The **Pause** icon appears dimmed if the data flow has been frozen. **NOTE:** On some pages, **Pause** and **Play** are the same icon that toggles between functions. That is, when clicked the: • **Pause** icon becomes the **Play** icon. • **Play** icon becomes the **Pause** icon.
Play		Unfreezes the data flow. The time and date refresh as soon as the data flow is updated. The **Play** icon appears dimmed if the data flow is live. **NOTE:** On some pages, **Pause** and **Play** are the same icon that toggles between functions. That is, when clicked, the: • **Pause** icon becomes the **Play** icon. • **Play** icon becomes the **Pause** icon.
Refresh		Updates the real-time data in a table, chart, or other display.
Resolve		Performs ARP or DNS resolution on MAC or FQDN entries: • **Resolve** for resolving one or more selected entries in the table • **Resolve All** for resolving all entries in the table

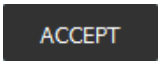
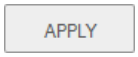
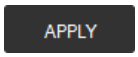
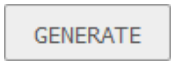
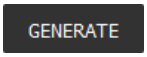
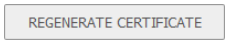
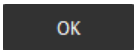
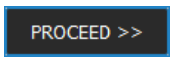
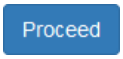
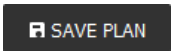
Display Icon

Many **INVESTIGATE** reports that display sometimes rapidly changing data have a **Display** icon associated with them. This icon is located at the top of the report page near the **Mode** option. Clicking on the icon opens a new tab in your browser that displays only that report. You can display all these reports or only the ones of interest. When the report is in a new tab, you can move the tab to a new browser window to display separately from the management interface.

Buttons

The management interface uses buttons to facilitate certain actions. Some buttons are common throughout the management interface while others apply to only one or two pages. Buttons describes the functions of the buttons used in the management interface:

Buttons

Action	Button	Description
Buttons that confirm and/or perform actions		
ACCEPT		Applies the changes entered on certain management interface pages.
ANALYZE		Starts analysis of the data in the table.
APPLY	 	Applies the changes made in a dialog or guide, but does not close the dialog.
CHANGE		Applies a change to a setting.
GENERATE	 	Generates the: • Configured settings. • Certificate signing request.
REGENERATE CERTIFICATE		Regenerates the self-signed HTTPS server certificate.
GO	 	Runs the diagnostic tool. Performs Botnet server lookup.
OK	 	Applies the changes entered on the management interface page or for a dialog, applies the changes and closes the dialog.
PROCEED		Applies the changes entered on the management interface page and acknowledges you accept the terms of the End User License Agreement (EULA). Continues with the **Mail Server Info Needed** dialog.
Proceed		Disables Cloud backup.
SAVE	 	Applies the changes made in a dialog or popup and then closes the dialog or popup.
SAVE PLAN		Saves the floor plan.

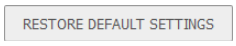
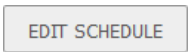
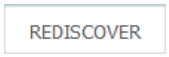
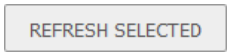
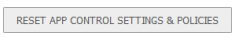
Buttons

Action	Button	Description
SAVE SELECTED	SAVE SELECTED	Saves the selected table or list entries.
SUBMIT	SUBMIT	Submits the request.
Buttons that start/stop actions		
RESTART	RESTART	Restarts the security appliance.
START	START	Starts a process running.
STOP	STOP	Stops a running process.
START CAPTURE	START CAPTURE	Captures all packets except those used for communication between the security appliance and the management interface on your console system.
STOP CAPTURE	STOP CAPTURE	Stops packet capture.
START DATA COLLECTION	START DATA COLLECTION	Starts data collection for logs.
START MIRROR	START MIRROR	Sends a copy of captured packets (mirroring) to another interface or to a remote SonicWall security appliance.
STOP MIRROR	STOP MIRROR	Stops sending captured packet mirroring.
Buttons that enable/disable		
ENABLE ALL	ENABLE ALL	Enables all Syslog servers.
DISABLE ALL	DISABLE ALL	Disables all Syslog servers.
ENABLE VLAN	ENABLE VLAN	Enables a custom VLAN ID on a specific trunk port.
Buttons for configuring		
ADVANCED	ADVANCED	Displays a dialog for configuring advanced DHCP server settings.
AUTO-CONFIGURE	AUTO-CONFIGURE	Displays a dialog for specifying auto-configuration for policy user authentication bypass.
CONFIGURE	CONFIGURE or CONFIGURE	Displays a configuration dialog for configuring SonicOS settings. **NOTE:** The **CONFIGURE** button(s) and **Configure** icon have different functions.
CONFIGURE APP CONTROL SETTINGS	CONFIGURE APP CONTROL SETTINGS	Displays a dialog for configuring an App Control rule.
CONFIGURE LDAP	CONFIGURE LDAP	Displays a dialog for configuring LDAP servers for authentication.
CONFIGURE RADIUS	CONFIGURE RADIUS	Displays a dialog for configuring RADIUS servers for authentication.
CONFIGURE SSO	CONFIGURE SSO	Displays a dialog for configuring SSO servers for authentication.

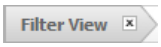
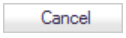
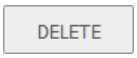
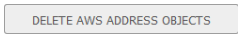
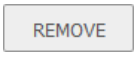
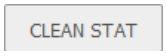
Buttons

Action	Button	Description
CONFIGURATION MODE	CONFIGURATION MODE	Places the security appliance in Configuration Mode, which allows changes to be made to SonicOS settings.
END CONFIG. MODE	END CONFIG. MODE	Places the security appliance in Non-Config. Mode, which prohibits changes to be made to SonicOS settings.
CONVERT TO NETWORK(S)	CONVERT TO NETWORK(S)	Allows tracked HTTPS destination IP addresses to be converted to a network for network bypass authentication.
EXT. SUPPORT SIGNED SMB	EXT.SUPPORT SIGNED SMB	Displays a dialog for configuring and enabling Extended Support for Signed SMB Acceleration.
NEW GROUP	NEW GROUP	Displays a dialog for configuring a port-mirroring group.
UNGROUP	UNGROUP	Deletes the mirrored group.
SCEP	SCEP	Displays a dialog for configuring SCEP.
	SCEP	Generates the configured SCEP.
SETTINGS	SETTINGS	Displays a menu for configuring an access point floor plan.
Buttons that add elements		
ADD	ADD	Displays a dialog that allows you to add elements, such as zones, services, and virtual access points, to your security appliance.
	ADD...	
ADD ALL	Add All	Moves all items from a generic list to a specific list.
ADD BOOKMARK	ADD BOOKMARK	Adds membership to the SSL VPN Services group and submits the change to enable adding bookmarks.
ADD COMPONENT	ADD COMPONENT	Displays a dialog for configuring components of a user-name attribute.
ADD DYNAMIC	ADD DYNAMIC	Displays a dialog for configuring a dynamic server lease range.
ADD STATIC	ADD STATIC	Displays a dialog for configuring a static server lease range.
ADD GROUP	ADD GROUP	Displays a dialog that allows you to add groups, such as user or DHCP option, to your security appliance.
ADD GUEST	ADD GUEST	Displays a dialog that allows you to configure guest user settings and services.
ADD OID	ADD OID	Adds an object ID for SNMP views.
ADD OPTION	ADD OPTION	Displays a dialog for configuring a DHCP option object.N
ADD SWITCH	ADD SWITCH	Displays a dialog for adding an X-Series switch.
ADD USER	ADD USER	Displays a dialog that allows you to add users to user groups.
AUTO ASSIGN	AUTO ASSIGN	Assigns items to the selected partition automatically.

Buttons

Action	Button	Description
NEW MAPPING		Creates a new Address Group mapping.
Buttons that edit elements or reset values		
DEFAULT		Discards all custom settings and restores default settings.
RESTORE DEFAULT SETTINGS		Discards all custom settings and restores default settings.
DEFAULT BLOCKED PAGE		Restores the default blocked page text.
EDIT		Displays a dialog (secondary or popup window) for editing the option.
EDIT SCHEDULE		Displays the **Edit Schedule** dialog for editing the **App Visualization Report** schedule.
EXAMPLE TEMPLATE		Reverts the HTML message code to the default HTML message.
REDISCOVER		Validates the topology is current by checking for changes to the wireless infrastructure.
REFRESH		Updates real-time data in a table.
		Updates real-time data in the tables on a page.
REFRESH DATA		Updates real-time data in the tables on a page.
REFRESH NOW		Reads mirrored groups from the server.
REFRESH SELECTED		Updates the data for the selected entries in a table.
REMOVE LAST		Deletes the last component of a user-name attribute.
RESET APP CONTROL SETTINGS & POLICIES		Resets all App Control settings and policy configuration to factory defaults.
RESET COUNTS		Clears the CloudWatch logs.
RESET DATA		Clears the data in the table and restarts data collection.
RESET QOS SETTINGS		Resets the 802.1p DiffServ conversion table values.
SET AS DEFAULT		Makes the selected WXA group the default WXA group.
UNSET DEFAULT		Clears the default WXA group.
SET TO ALL		Sets all entries in a table to the specified operation or setting.

Buttons

Action	Button	Description
Buttons that filter data		
CONVERT TO WILDCARD		Allows wildcard matching for bypass authentication.
FILTER		Filters the table entries based on specified criteria.
FILTER ADD		Adds the selected element to the filter
Filter View		Adds or deletes a filter based on selected criteria.
SELECT		Displays a popup dialog for choosing variants.
Buttons that cancel or delete		
CANCEL	 	Discards the changes entered on the management interface page or for a dialog, discards any changes made in the dialog and closes the dialog.
CLOSE		Discards any changes made in the dialog and closes the dialog.
Close Search		Closes the open global search results, but does not delete the results.
DELETE	 	Deletes the selected item(s) from a table. Deletes the item, especially in a filter.
DELETE ALL		Deletes all entries except default and system-generated items in a table.
DELETE AWS ADDRESS OBJECTS		Deletes all AWS-related Address Objects and Groups.
DELETE COOOKIES		Deletes all cookies saved by the SonicWall security appliance and clears any choices remembered in the browser.
DELETE SELECTED		Deletes the selected entries from the table.
EXCLUDE		Excludes entries in the connection failure list.
EXIT GUIDE		Closes the guide without saving changes.
REMOVE		Deletes the selected item(s) from a table.
REMOVE ALL	 	Deletes all items in a table or list.
UNDO		Clears the changes and reverts the data in the list to original settings.
CLEAN STAT		Cleans all policy statistics.

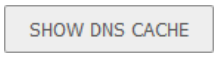
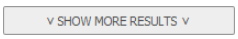
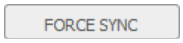
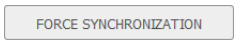
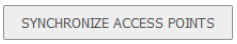
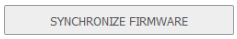
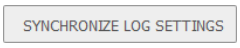
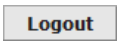
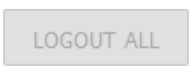
Buttons

Action	Button	Description
Buttons that clear or flush data		
CLEAN STAT	CLEAN STAT	Cleans all policy statistics.
CLEAR	CLEAR	Clears table information such as: • Packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging. • Historical RF monitoring information. • Connection failure list entries.
	CLEAR	Clears selected Connection failure list entries.
CLEAR ALL	CLEAR ALL	Clears all Connection failure list entries.
CLEAR STATS CLEAR STATISTICS	CLEAR STATS CLEAR STATISTICS	Clears the counters and the displayed statistics; restarts the counters.
CLEAR DATA	CLEAR DATA	Clears the data in the Flow Reporting Statistics tables.
FLUSH	FLUSH	Removes one or more selected items in a table.
FLUSH ALL	FLUSH ALL	Removes all items in a table.
FLUSH ARP CACHE	FLUSH ARP CACHE FLUSH ARP CACHE	Flushes the ARP cache and updates the configuration.
FLUSH NDP CACHE	FLUSH NDP CACHE FLUSH NDP CACHE	Flushes the NDP cache and updates the configuration.
Buttons for importing/exporting and uploading files		
Browse	Browse... Browse ...	Displays an explorer window for selecting a file.
DOWNLOAD REPORT	DOWNLOAD REPORT	Generates a detailed report of the SonicWall security appliance configuration and status and saves the report to the local hard disk.
EXPORT	EXPORT	Exports table contents to a file.
IMPORT	IMPORT IMPORT	Imports table contents or a certificate from a file.
IMPORT EXCLUSIONS	IMPORT EXCLUSIONS	Displays a dialog for selecting a default exclusion database to import.
IMPORT SIGNATURES	IMPORT SIGNATURES	Displays a dialog for selecting a signature file to import.

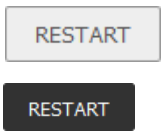
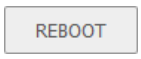
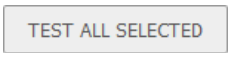
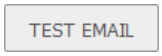
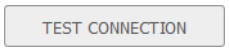
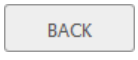
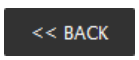
Buttons

Action	Button	Description
IMPORT USERS	IMPORT USERS	Displays a popup dialog for importing users from a server.
IMPORT USER GROUPS	IMPORT USER GROUPS	Displays a popup dialog for importing user groups from a server.
LOAD FROM FILE	LOAD FROM FILE	Imports table or list contents from a file.
READ FROM SERVER	READ FROM SERVER	Displays a popup dialog for reading the server's schema and then either updating the server's schema or exporting the schema.
SEND DIAGNOSTIC REPORTS TO SUPPORT	SEND DIAGNOSTIC REPORTS TO SUPPORT	Send the TSR, system preferences, and trace log to SonicWall Engineering (not to SonicWall Technical Support).
UPLOAD	UPLOAD	Uploads a certificate file.
Upload a file	Upload a file	Uploads a snapshot of the page to a pdf file.
Buttons for monitoring and logging		
LOG NOW	LOG NOW	Tests the connection to the FTP server and transfers the capture buffer contents to the server.
LOG TO FTP SERVER	LOG TO FTP SERVER	Sends a log of capture data to an FTP server.
MONITOR ALL	MONITOR ALL	Resets current monitor filter settings and advanced page settings so that traffic on all local interfaces is monitored.
MONITOR DEFAULT	MONITOR DEFAULT	Resets current monitor filter settings and advanced page settings to factory default settings.
SEND ALL ENTRIES	SEND ALL ENTRIES	Sends the necessary fields of log settings to the external collector for log display.
Buttons for showing/generating data		
GENERATE ALL TEMPLATES	GENERATE ALL TEMPLATES	Generates templates for external collectors.
GENERATE STATIC APPFLOW DATA	GENERATE STATIC APPFLOW DATA	Generates static Appflow data.
Global Search		Displays the Global Search function. **NOTE:** The **Search** button and the **Search** icon have different functions.
HELP	HELP	Displays the online help page for the dialog.
NEW SIGNING REQUEST	NEW SIGNING REQUEST	Displays a dialog for generating a certificate signing request.
PREVIEW	PREVIEW	Displays the HTML message in a dialog for verification of how the message looks.
SCAN ALL	SCAN ALL	Scans all entries in a table.
SHOW BOTNETS	SHOW BOTNETS	Displays a popup containing resolved Botnet locations.
SHOW CACHE	SHOW CACHE	Displays a popup containing cache statistics.

Buttons

Action	Button	Description
SHOW CONNECTION FAILURES		Displays a popup listing connection failures.
SHOW DNS CACHE		Displays a popup containing DNS cache statistics.
SHOW LESS RESULTS		Displays only the top 10 results of a global search.
SHOW LOG MONITOR		Displays the **INVESTIGATE | Logs | Event Logs** page.
SHOW MORE RESULTS		Displays all the results of a global search.
SHOW REVERSE DNS CACHE		Displays a popup containing reverse DNS cache statistics.
Buttons for synchronizing data/security appliances		
FORCE SYNC		Forces an immediate synchronization of logs between SonicOS and Amazon's AWS.
FORCE SYNCHRO-NIZATION		Forces synchronization of Address Objects and Groups with Amazon AWS according to saved mappings.
SYNCHRONIZE	 	Synchronizes the licenses of the security appliance with those on `www.sonicwall.com`.
SYNCHRONIZE ACCESS POINTS		Synchronizes SonicPoints and SonicWaves of the security appliance.
SYNCHRONIZE FRIMWARE		Synchronizes the firmware of the primary and secondary security appliances in a high availability pair.
SYNCHRONIZE LOG SETTINGS		Sends the necessary fields of log settings to the GMSFlow server for log displaying.
SYNCHRONIZE SERVER		Sends static GMSFlow data to the GMSFlow server.
SYNCHRONIZE SETTINGS		Synchronizes the configuration of the primary and secondary security appliances in a high availability pair.
Buttons for controlling the security appliance		
FORCE ACTIVE/STANDBY FAILOVER		Forces active/standby failover in the primary and secondary security appliances in a high availability pair.
LOGOUT		Logs out the: • Selected users in the table from the system. • Admin from SonicWall Virtual Office.
LOGOUT ALL		Logs out all users in the table from the system.
LOGOUT SELECTED USERS		Logs out all selected users in the table from the system.

Buttons

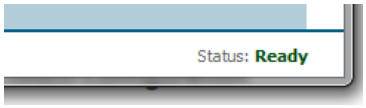
Action	Button	Description
RESTART		Restarts the security appliance.
REBOOT		Reboots the selected object(s) in the table.
REBOOT ALL		Reboots all objects in the table.
Buttons for testing		
PROBE ALL		Probes all WXA series appliances.
RESOLVE		Resolves the spoof detected list.
TEST		Test the settings on the server.
TEST ALL SELECTED		Tests multiple entries selected in the table.
TEST DETAILS		Displays the tests if the test of the connection to Amazon's AWS contained any errors.
TEST EMAIL		When Send Report by Email is enabled, sends a test report to the email address.
TEST CONNECTION		Tests the connection to Amazon's AWS and displays any errors.
TEST CONNECTIVITY		Connects to the GMSFlow server to gather registration information, image version, and counters.
TEST SETTINGS		Sends a test connection to the configured mail server.
Buttons for PortShield		
HIDE PORTSHIELD INTERFACES		Hides portshielded interfaces from display in the table.
PORTSHIELD WIZARD		Displays the PortShield Guide.
SHOW PORTSHIELD INTERFACES		Shows portshielded interfaces from display in the table.
Buttons for navigation		
BACK		Displays the previous page of the guide.
		
NEXT		Displays the next page of the guide.
		

Buttons

Action	Button	Description
LEFT ARROW	<- <-	Removes an item from a specific list to a generic list.
RIGHT ARROW	-> ->	Moves an item from a generic list to a specific list.

Status bar

The **Status** bar at the bottom of the management interface window displays the status of actions executed in the management interface. If the action was not completed, the **Status** bar displays an error message.



Applying Changes

Click **ACCEPT** to save any configuration changes you made on the page.

If the settings are contained in a dialog (secondary window) within the management interface, the settings are applied automatically to the security appliance when you click **OK**. To apply the settings without closing the dialog, some dialogs have an **APPLY** button.

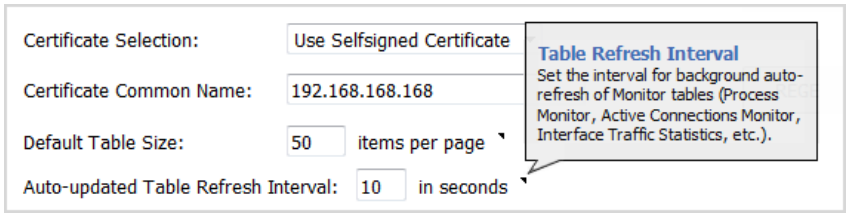
To cancel any configuration changes before applying them, click **CANCEL**.

Tooltips

Topics:

Generic Tooltips

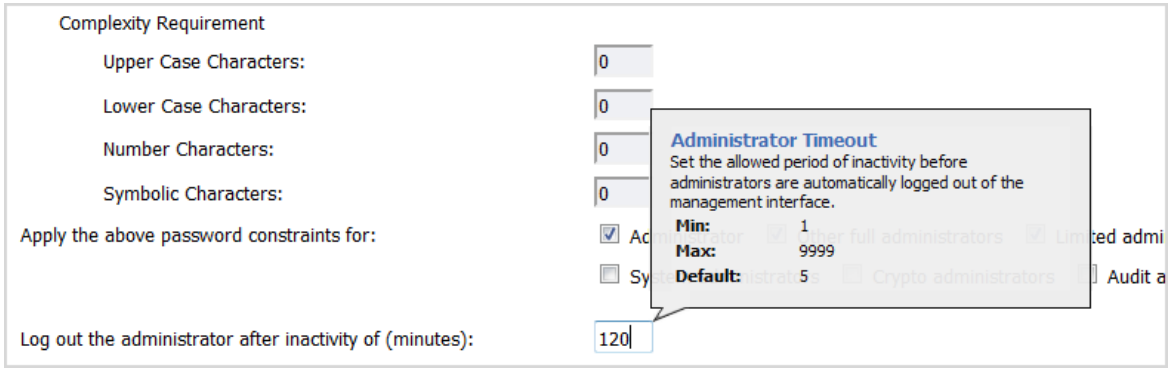
SonicOS provides embedded tooltips, or small popup balloons, that display when you hover your mouse over an element in the management interface or click on a small triangle after the element. They provide brief information describing the element. Tooltips are displayed for many forms, buttons, table headings, and entries.



NOTE: Not all management interface elements have Tooltips. If a Tooltip does not display after hovering your mouse over an element for a couple of seconds, you can safely conclude that it does not have an associated Tooltip.

Tooltips with Values

When applicable, Tooltips display the minimum, maximum, and default values for form entries. These entries are generated directly from the SonicOS firmware, so the values are correct for the specific platform and firmware combination you are using.

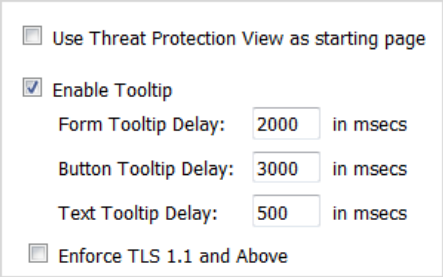


Several tables include a tooltip that displays the maximum number of entries that the security appliance supports. For example, **MANAGE | PoliciesPolicies | Address Objects** displays the maximum number of address groups the security appliance supports. These entries are generated directly from the SonicOS firmware, so the values are correct for the specific platform and firmware combination you are using.

Tables that display the maximum entry tooltip include NAT policies, access rules, address objects, and address groups.

Configuring Tooltips

The behavior of the Tooltips are configured in the **Web Management Settings** section of **MANAGE | System Setup System > Appliance > Base Settings**.



Tooltips are enabled by default. To disable Tooltips, clear **Enable Tooltip**. The duration of time before Tooltips display can be configured:

This option	Configures the duration, in milliseconds, before Tooltips display for
Form Tooltip Delay	Forms (fields where you enter text)
Button Tooltip Delay	Radio buttons and checkboxes
Text Tooltip Delay	Management Interface text

Manipulating Tables

Topics:

Navigating Dynamic Tables

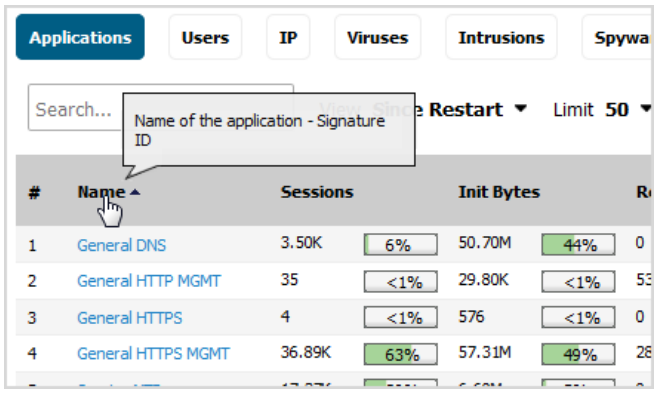
In the SonicOS dynamic Management Interface, table statistics and log entries dynamically update without requiring you to reload your browsers.You can navigate tables in the management interface with a large number of entries by using the navigation buttons located on the upper-right corner of the table. The table navigation bar includes buttons for moving through table pages:

You can specify the default table size (number of items per page) in the **Web Management Settings** section of **MANAGE | System Setup > Appliance > Base Settings**

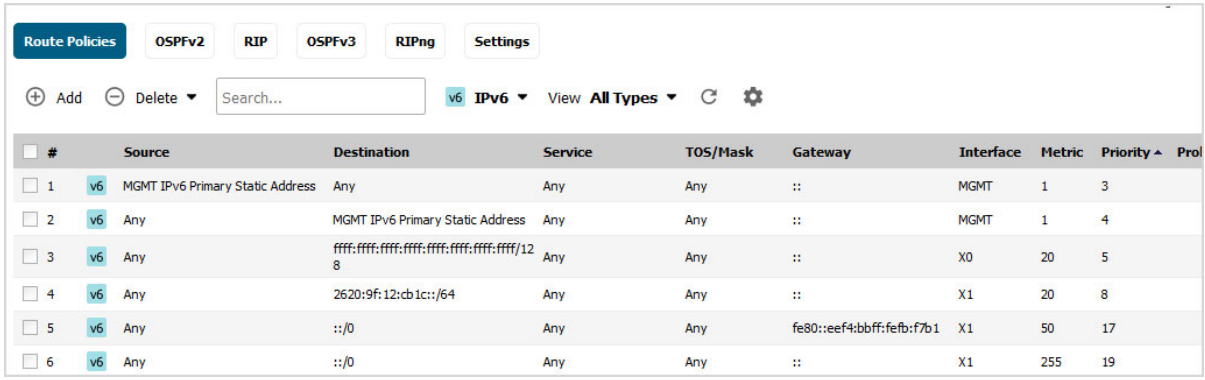
Sorting Tables

Tables are sorted automatically by the first column of data (not the **#** column). Many tables can be re-sorted by clicking on the headings for the various columns. On tables that are sortable, the cursor becomes a pointing

hand when you mouse over the column headings. A small upward or downward triangle indicates the column on which the table is sorted and the direction of the sort.

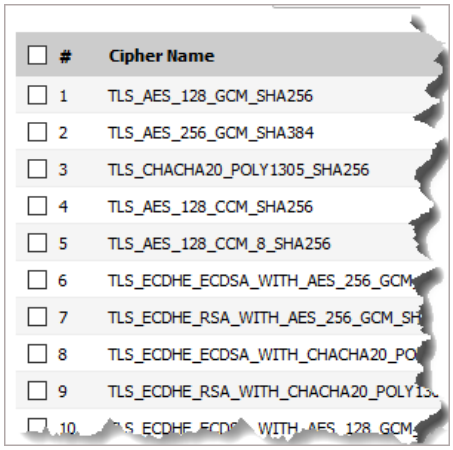


When tables are sorted, entries with the same value for the column are grouped together with the common value shaded as a sub-heading. In the following example, the **Route Policies** table is sorted by **Priority**.



Selecting Table Entries

Many tables allow you to select table entries for deleting, flushing, blocking, and other actions. Tables that allow you to do so start each row (entry) with a checkbox and usually a number:



To select one or more entries:

1. Click the checkbox(es) of the entry/entries.
2. Perform the action.

To select all entries at once:

1 Click the checkbox in the table header.

2 Perform the action.

Removing Table Entries

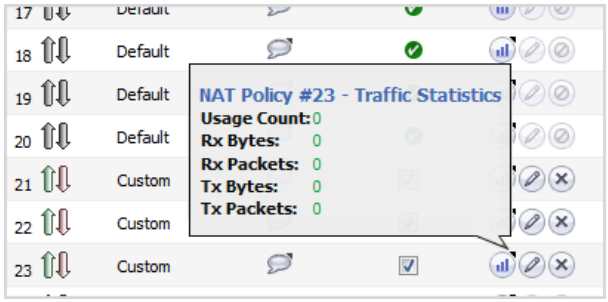
Active connections, user sessions, VoIP calls, and similar activities can be disconnected or flushed dynamically with a single click on the **Delete** icon in the **Flush** or **Logout** column.

To flush one or more selected items in the table, click the **FLUSH** button. To flush all the items in the table, click the **FLUSH ALL** button.

To delete FQDN objects from a table, select from the **Purge** drop-down menu:

- **Purge** to delete one or more selected objects.
- **Purge All** to delete all the objects from the table.

Displaying Statistics



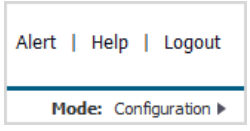
Several tables include a table **Statistics** icon that displays a brief, dynamically updating summary of information for that table entry. Some tables with the **Statistics** icon are:

- **Port Configuration** on the **MANAGE | System Setup | Network > PortShield Groups** page
- **NAT Policies** on the **MANAGE | PoliciesPolicies | Rules > NAT Policies** page
- **Relay Protocols** on the **MANAGE | System Setup |Network > IP Helper** page
- **Access Rules** on the **MANAGE | PoliciesPolicies | Rules > Access Rules** page
- **App Rules Policies** on the **MANAGE | PoliciesPolicies | Rules > App Rules** page

To update the real-time data in a table, click the **Refresh** icon or the **REFRESH** button.

To clear the statistics and start statistics collection anew, click the **CLEAR STATISTICS** button.

Management Interface Options



The top-right corner of every management interface page has the following options that you can click:

- Help on page 39

- Logout on page 39
- Mode on page 39

Help

Each security appliance includes Web-based online help that explains how to use management interface pages and how to configure the security appliance. Clicking **help** accesses the context-sensitive help for the page.

Some of the dialogs also have a **HELP** button that accesses context-sensitive help for the window.

Logout

Each firewall includes a **Logout** option that terminates the management interface session and displays the authentication page for logging into the firewall. Clicking **Logout** logs you out of the firewall.

Mode

Each appliance includes a **Mode** option that toggles the configuration mode of the management interface between:

- **Configuration** mode – You can make changes to the settings of the SonicWall security appliance.
- **Non-Config** mode – You can only view the settings of the security appliance and cannot make any changes or view some management interface pages.

The mode option allows you to toggle between configuration mode and non-configuration mode.

To change mode:

1 Click the arrow next to **Mode: Configuration**/**Mode: Non-Config**. The display changes:

2 Click **Change mode**. The mode and display change.

You can also change mode on the **MANAGE | System Setup > Appliance > Base Settings** page.

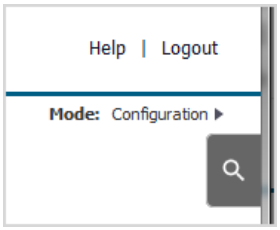
Using Global Search

NOTE: The global search feature is not available in the classic/legacy management interface.

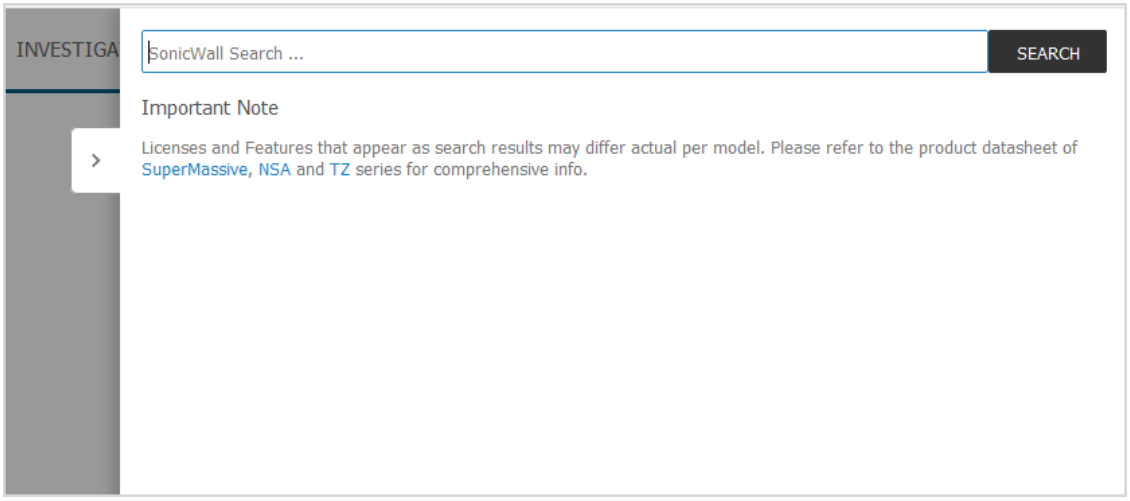
SonicOS provides a global search feature that makes it easy for you to navigate to desired data. Results contain links to main pages that are part of menu items in the navigation pane and to online help. Only static data can be searched; dynamic data, such as object names and policy details, cannot. The feature is available on all management interface pages except for the Quick Configuration guides.

To perform a global search:

1 On any management interface page, click the **Global Search** button:



The **Search** function expands.



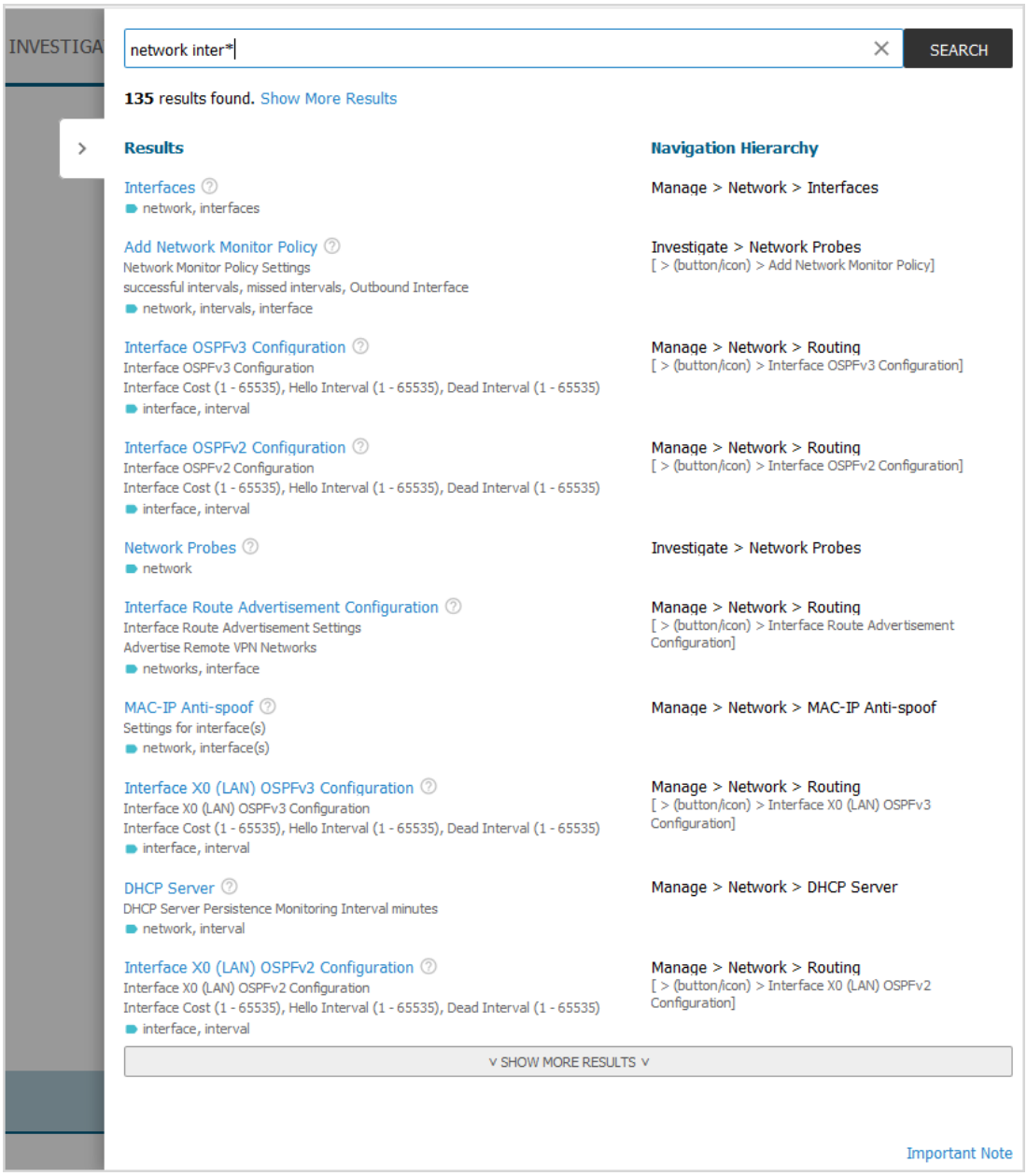
2 Enter a query in the **Search** field:

- Single word queries; for example, `ARP`
- Multi-word queries; for example, `Network Interface`; search results are determined by performing an OR operation on search terms.
- Queries with the `*` wildcard; for example, `Network Inter*`

You can enter up to 50 alphanumeric (A-Z, a-z, 0-9) and special (. -_ / *) characters. The query is not case sensitive.

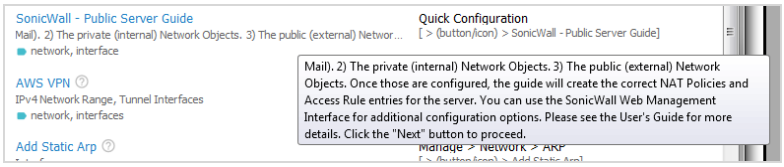
Only pages displayed in the **Navigation** pane are searched.

The search results display along with the number of results.



IMPORTANT: Search results for licenses and features may differ depending on the model of the security appliance. For more information, see the datasheet(s) for your security appliance(s).

The results are displayed in two columns:

Results	Contains: • A link to the management interface page containing the result. • An **Information** icon that, which clicked, displays the relevant online help. • Where, on the management interface page or one of its dialogs, the search results were found. Mousing over the location displays a popup with more detail about the location:  • A listing of the search criterion or criteria found (for example, `Network Interf*` returns network, networks, networking, interface, interface(s), and interfaces when found).
Navigation Hierarchy	Displays the navigation to the management interface page containing the search criteria and, if relevant, the dialog containing the search criteria: 

TIP: Clicking the link to the management interface page displays the main page even if the search result is a popup displayed from within the main page.

3 By default, the 10 most relevant results are displayed. If there are more than 10 results, a link, **Show More Results**, displays next to the number of results found and a **SHOW MORE RESULTS** button appears at the bottom of the page. Clicking either displays all the results and a slider for navigation.

4 To close the search results:

- Click the **Close** button.
- Click outside the search results.
- Press the **Esc** key.

NOTE: Closing the search results does not remove them. If you display the search feature again from any page, the search results redisplay. To delete the search results, clear the **Search** field.

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://support.sonicwall.com.

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, refer to https://support.sonicwall.com/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.

SonicOS 6.5 About SonicOS
Updated - February 2019
Software Version - 6.5.4
232-002578-04 Rev A