About SonicOS 8

Contents

What is SonicOS? **3**
Where Do I Find Information About SonicOS? 3
Web Management to Admin Guides Reference 4

About the SonicOS Management Interface **8**
Logging Into SonicOS 8
Logging Out of SonicOS 9
About the Top Menu Views 10
About the API and CLI 11
Legal Information 13
SonicOS Guides (Wizards) 14
Notification Center 14
Online Help 16
Global Search 16

SonicWall Support **19**
About This Document 20

1

What is SonicOS?

SonicOS 8 runs on SonicWall network security appliances (firewalls) and provides a web management interface for configuring the features, policies, and security services, updating the firmware, managing connected devices such as switches and access points, monitoring traffic/users/threats, investigating events, and much more. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

SonicOS provides a modern graphical management interface that facilitates:

- Setting up and configuring your security appliance
- Monitoring the health and status of the security appliance, network, users, connections and the status of the incoming and outgoing traffic
- Configuring external devices, such as access points or switches

SonicOS also provides full-featured API and a command-line interface (CLI) in addition to the graphical management interface. For more information, see About the API and CLI.

For information about the SonicOS management interface, see About the SonicOS Management Interface.

Where Do I Find Information About SonicOS?

SonicOS administration guides are available for each main menu in the left navigation pane of the SonicOS web management interfaces. Within each guide, you will find topics covering each page in that menu group, with procedures and detailed information.

SonicOS administration guides are published on the SonicWall Technical Documentation portal at: https://www.sonicwall.com/support/technical-documentation/?language=English&category=Firewalls.

On the left side of the page, you can select SonicOS or the firewall series of your choice. Scrolling down on the left, you can select the type of document and then the firmware version, followed by the virtual platform, date range, and language.

For example, the *SonicOS 8 Tools & Monitors* administration guide covers the following main topics:

- Using Packet Monitor
- Viewing Connections
- Monitoring Core 0 Processes
- Using Packet Replay

For a mapping of SonicOS 8 web management interface sections to the SonicOS 8 administration guides, refer to SonicOS Web Interface to Administration Guide Reference.

Web Management to Admin Guides Reference

Management Interface Section	Guide Name	Topics Covered
HOME | Dashboard	SonicOS 8 Dashboard	Describes the key information and actionable features of the four Dashboard System screens: Status, Summary, Network and Threat. Covers the Access Points dashboard for SonicWave and SonicPoint, and provides information about the Capture ATP page. Describes the Topology page with the network topology graphical display.
HOME | Legal Information HOME | API Wizards button in top banner Login/Logout screens	SonicOS 8 About SonicOS	Describes the Legal Information page and API page with Swagger access. Provides an overview of available wizards and of the SonicOS Login and Logout screens. Also describes some new features and the set of admin guides.
MONITOR | Real-Time Charts	SonicOS 8 Real-Time Charts	Describes real-time charts for System Monitor, Protocol Monitor, Users Monitor, and Bandwidth Management (BWM) Monitor.
MONITOR | AppFlow	SonicOS 8 Monitor AppFlow	Describes the AppFlow Report and Appflow Monitor pages.
MONITOR | SDWAN	SonicOS 8 SDWAN	Describes the SDWAN Monitor and SDWAN Connections pages.
MONITOR | Logs	SonicOS 8 Monitor Logs	Describes the System Logs and Auditing Logs pages.
MONITOR | Tools & Monitors	SonicOS 8 Tools & Monitors	Covers using Packet Monitor, viewing Connections, monitoring Core 0 Processes, and using Packet Replay.
DEVICE | Settings	SonicOS 8 Settings	Configuration options and procedures for security service and support licenses, administration settings, system time settings, certificates, SNMP settings, firmware backups, upgrade, bootup options, and configuration settings export and import, and restarting the firewall.
DEVICE | High Availability	SonicOS 8 High Availability	Configuration options and procedures for High Availability settings. Describes HA status.

Management Interface Section	Guide Name	Topics Covered
DEVICE | Users	SonicOS 8 Users	Configuration options and procedures for adding local users and groups, guest accounts and services. Describes viewing status of local and guest users.
DEVICE | AppFlow	SonicOS 8 Device AppFlow	Configuration options and procedures for Flow Reporting and AppFlow Agent. Configuring, generating and downloading the Capture Threat Assessment Report.
DEVICE | Log	SonicOS 8 Device Log	Configuration options and procedures for log settings, syslog, automation, name resolution, reports, and AWS.
DEVICE | Diagnostics	SonicOS 8 Diagnostics	Configuration options and procedures for system diagnostics, including the Tech Support Report (TSR), network settings, DNS lookup and reverse name lookup, network paths, using ping, using trace route, real-time blacklist, Geo-IP and botnet, MX and banner, GRID check, making a URL rating request, PMTU discovery,and terminal access.
DEVICE | Switch Network	SonicOS 8 Switch Network	Description of graphical views of the Switch network. Configuration options and procedures for adding and configuring SonicWall Switches.
DEVICE | Access Points	SonicOS8 Access Points	Configuration options and procedures for wireless access point settings, firmware management, using the floor plan view, intrusion detection (IDS), advanced intrusion and preventions (IDP), packet capture for wireless traffic, virtual access points, radio frequency monitoring and spectrum, Fairnet, WiFi multimedia, 3G/4G/LTE WWAN, Bluetooth, radio resource management. Describes viewing station status.
DEVICE | WWAN	SonicOS8 WWAN	Covers 4G/LTE WWAN modem and network status, viewing signal strength, and accessing the modem for monitoring and configuration.
NETWORK | System	SonicOS 8 System	Configuration options and procedures for system networking settings, including interfaces, failover and load balancing, neighbor discovery, ARP, MAC IP anti-spoof, web proxy, PortShield groups, VLAN translation, IP helper, dynamic routing, DHCP server, multicast, network monitor, and AWS configuration.
NETWORK | Firewall	SonicOS 8 Network Firewall	Configuration options and procedures for advanced firewall settings, DoS flood protection, SSL control, cipher control, and real-time-blacklist filter.

Management Interface Section	Guide Name	Topics Covered
NETWORK | VoIP	SonicOS 8 VoIP	Configuration options and procedures for voice over IP settings. Viewing call status and controlling calls.
NETWORK | DNS	SonicOS 8 DNS	Configuration options and procedures for Domain Name Service settings, dynamic DNS, DNS proxy, and DNS security.
NETWORK | SDWAN	SonicOS 8 SDWAN	Configuration options and procedures for SDWAN groups, SLA probes, SLA class objects, path selection profiles, and SDWAN rules.
NETWORK | IPSec VPN	SonicOS 8 IPSec VPN	Configuration options and procedures for IPSec VPN rules and settings, advanced settings, DHCP over VPN, Layer 2 Tunneling Protocol server, and AWS VPN.
NETWORK | SSL VPN	SonicOS 8 SSL VPN	Configuration options and procedures for SSLVPN server, client, and portal settings. Describes Virtual Office portal access and viewing SSL VPN status.
OBJECT | Match Objects	SonicOS 8 Match Objects	Configuration options and procedures for objects to be used in policy rules, including object types for zones, addresses, services, URI lists, match objects, schedules, dynamic groups, and email addresses.
OBJECT | Profile Objects	SonicOS 8 Profile Objects	Configuration options and procedures for profile objects to be used in policy rules, including profile objects for endpoint security, bandwidth, quality of service marking, content filtering, DHCP option, and AWS.
OBJECT | Action Objects	SonicOS 8 Action Objects	Configuration options and procedures for action objects to be used in policy rules, including app rule actions and content filter actions.
POLICY | Rules and Policies	SonicOS 8 Rules and Policies	Configuration options and procedures for access rules, NAT rules, routing rules, content filter rules, app rules, and endpoint rules.
POLICY | DPI-SSL	SonicOS8 DPI-SSL	Configuration options and procedures for client and server DPI-SSL.
POLICY | DPI-SSH	SonicOS8 DPI-SSH	Configuration options and procedures for DPI-SSH settings.
POLICY | Security Services	SonicOS8 Security Services	Configuration options and procedures for licensed security services, including Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Geo-IP Filter, Botnet Filter, App Control, and Content Filter. Describes viewing the summary of security services status.
POLICY | Anti-Spam	SonicOS8 Anti-Spam	Configuration options and procedures for Anti-Spam settings. Describes viewing Anti-Spam status.

Management Interface Section	Guide Name	Topics Covered
POLICY | Capture ATP	SonicOS 8 Capture ATP	Configuration options and procedures for Capture ATP settings and viewing Capture ATP scanning history.
POLICY | Endpoint Security	SonicOS 8 Endpoint Security	Configuration options and procedures for endpoint (client) security.

2

About the SonicOS Management Interface

SonicOS 8 is designed for higher security, improved workflow and scalability, and a better user experience and ease of use.

This section introduces these top-level interface features:

Topics:

- Logging Into SonicOS
- Logging Out of SonicOS
- Contemporary vs Classic Web Interface
- Global Search
- Online Help
- Notification Center
- SonicOS Guides (Wizards)
- SSH Terminal Access
- About the Top Menu Views
- About the API and CLI
- Legal Information

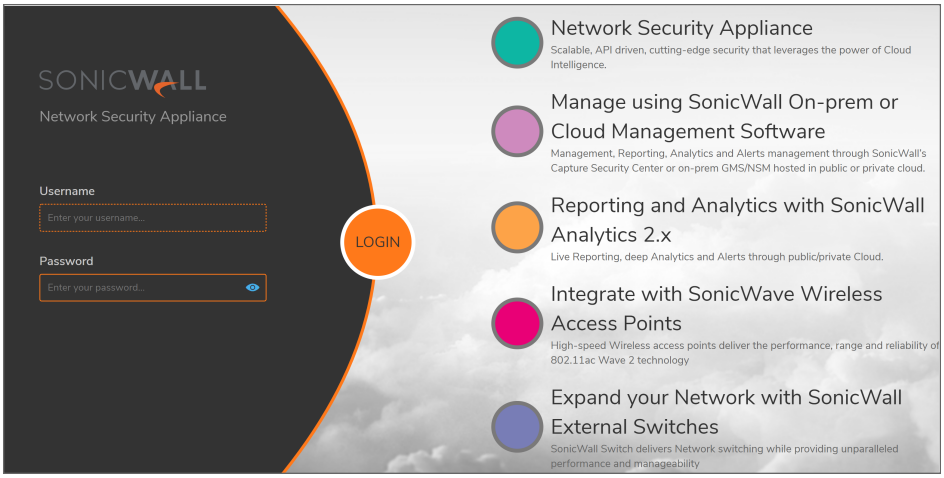
Logging Into SonicOS

To log into the SonicOS web management interface, enter the firewall IP address into your browser using HTTPS. The default X0 LAN IP address is https://192.168.168.168. The default credentials are:

- Username: *admin*
- Password: *password*

You can also log in using the WAN IP address if the WAN interface (usually X1 or X2) is configured to allow HTTPS management. SonicOS provides a DHCP server to give your computer an IP address in the same subnet, so there is no need to give it a static IP address before logging in.

The login page provides links to related SonicWall products at the right while you enter your SonicOS credentials at the left.

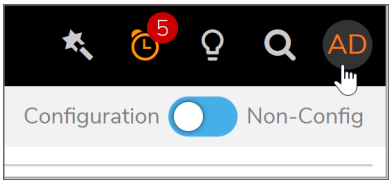


After entering the **Username** and **Password**, click **LOGIN** or press **Enter** to log in.

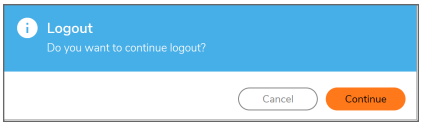
ⓘ | **NOTE:** The SonicOS web management interface is best viewed using 1920x1080 resolution.

Logging Out of SonicOS

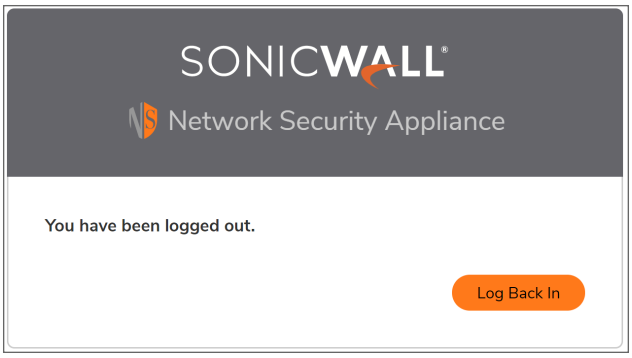
To log out of the SonicOS web management interface, click on the username initials at the top right corner of the banner and select **Logout** from the drop-down list.



In the confirmation dialog, click **Continue**.



The logout page is displayed.

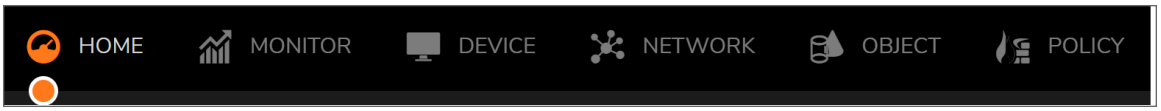


To log back into the firewall, click **Log Back In**.

For security reasons, SonicOS automatically logs the administrator out after a specified period of inactivity. The default inactive time is 5 minutes. To change this duration, configure the desired number of minutes in the **Log out the Admin after inactivity of (mins)** field in the **Login / Multiple Administrators** screen on the **DEVICE | Settings > Administration** page.

About the Top Menu Views

The contemporary SonicOS 8 web management interface layout is organized into high-level, intuitive workflows, with six top-level views in a menu across the top.



The currently selected top view is marked with an orange dot. A similar orange dot marks the currently selected page in the left navigation pane.

The six top-level views are:

View	Description
HOME	The **HOME** view provides dashboards and graphs designed to help you quickly see the health and security status of your security appliance, connected devices, and networks. In SonicOS, the Policy Overview page provides status information for your policies. On NSsp 13700 and TZ, NSa and NSv series, a graphical representation of your network topology is available in the HOME view. The API and Legal pages are also in the HOME view.
MONITOR	The **MONITOR** view provides Real-Time Charts, AppFlow reports and/or monitoring, AppFlow sessions (on NSv), Capture Threat Assessment report, SDWAN monitoring, system logs, and tools for packet capture and monitoring connections and processes.

View	Description
DEVICE	The **DEVICE** view provides configuration pages for firewall administration and settings, internal wireless settings for TZ wireless firewalls, high availability, users, AppFlow settings, log settings, and system diagnostic tools. In SonicOS, the Policy Lookup page is available under Diagnostics. On TZ, NSa and NSsp 13700 firewalls, configuration pages for external devices such as the SonicWall Switch, Access Points, and WWAN 4G/LTE are available.
NETWORK	The **NETWORK** view provides System configuration pages for network interfaces and system settings including for load balancing, ARP, web proxy, PortShield (on TZ and NSa series), VLAN translation, dynamic routing, DHCP server, etc, as well as pages for advanced firewall settings, VoIP, DNS, SDWAN, IPSec VPN, and SSL VPN settings.
OBJECT	The **OBJECT** view provides configuration pages for Match Objects, Profile Objects, and Action Objects, which are used when creating rules and policies on the **POLICY** view. In SonicOS, the OBJECT view provides configuration pages for Match Objects, Profile Objects, and Action Profiles, which are used when creating rules and policies on the **POLICY** view. A Signatures page allows refresh of Anti-Virus and Anti-Spyware signature databases on the firewall.
POLICY	The **POLICY** view provides menu groups for Rules and Policies, Capture ATP, and EndPoint Security. In SonicOS, the **POLICY** view provides those menu groups plus four additional ones: DPI-SSL, DPI-SSH, Security Services and Anti-Spam. The configuration pages include Access Rules, NAT Rules, Routing Rules, Content Filter Rules, App Rules and Endpoint Rules. The Settings page provides status for all security services on a single page, while the services are configured within each policy as an integral component. The Shadow page shows which rules are being shadowed by other rules and which rules are shadowing other rules. If a rule is shadowed by another rule, the first rule might never be hit.

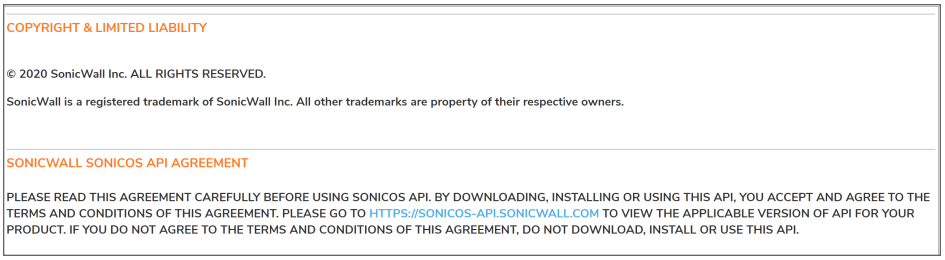
About the API and CLI

The SonicOS Enterprise Command Line Interface (E-CLI) provides a concise and powerful way to configure SonicWall security appliances without using the SonicOS web management interface. You can use the CLI commands individually on the command line or in scripts for automating configuration tasks. You can access the CLI by connecting to the Console port via SSH or with a serial connection. For more information, refer to the *SonicOS 8 Command Line Interface Reference Guide* on the SonicWall technical documentation portal.

The SonicOS RESTful API (Representational State Transfer Application Program Interface) provides an alternative method to the SonicOS CLI for configuring the firewall. You can use the API to configure each and every feature on the firewall or to script configuration sequences.

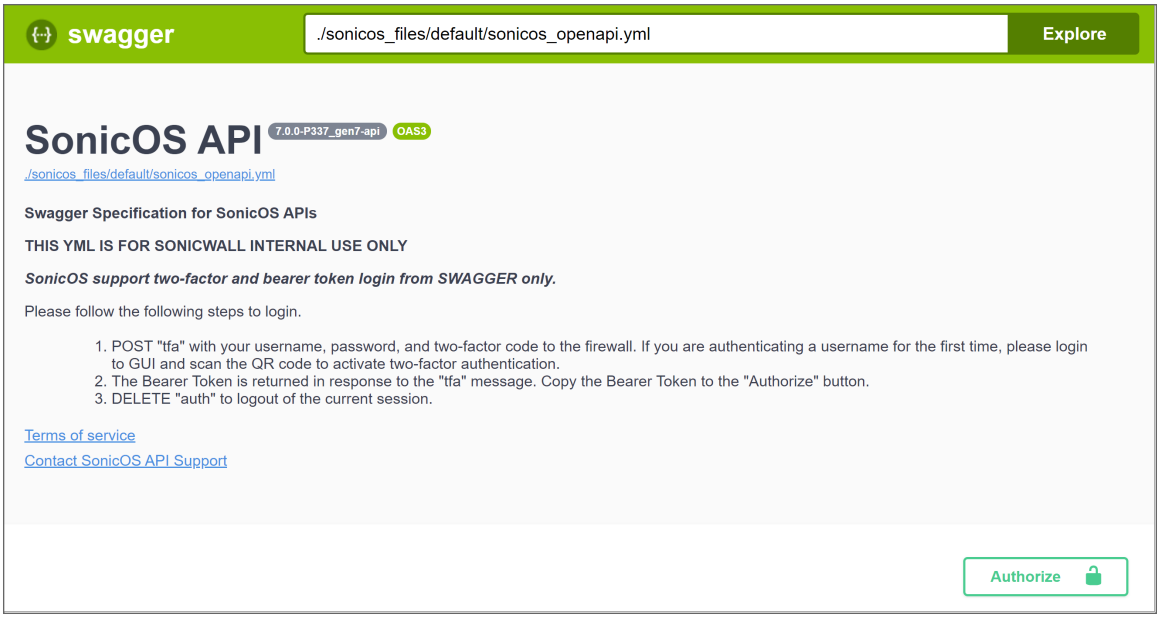
For more information, see the *SonicOS 7 API Reference Guide* on the SonicWall technical documentation portal.

To access the API, navigate to **HOME | API** and click the link in the **SONICWALL SONICOS API AGREEMENT** section.



You can also enter the link directly into your browser, https://sonicos-api.sonicwall.com.

The SonicOS API Swagger access page is displayed.



Set up your authentication and log in for the complete API command list and syntax.

```
openapi: "3.0.0"

info:
  description: |
    __Swagger Specification for SonicOS APIs__

    __THIS YML IS FOR SONICWALL INTERNAL USE ONLY__

    ___SonicOS support two-factor and bearer token login from SWAGGER only.___

    Please follow the following steps to login.
    > 1. POST "tfa" with your username, password, and two-factor code to the firewall. If you are authenticating
    > 2. The Bearer Token is returned in response to the "tfa" message. Copy the Bearer Token to the "Authorize"
    > 3. DELETE "auth" to logout of the current session.

  version: 7.0.0-R370_gen7-api
  title: "SonicOS API"
  termsOfService: "http://help.sonicwall.com/help/sw/eng/7621/8/0/0/content/app-license_agreement.65.2.htm"
  contact:
    name: "SonicOS API Support"
    email: "sonicOsApiSupport@SonicWall.com"
servers:
  - url: "https://{IP}:{PORT}/api/sonicos"
    description: "SonicWALL Appliance"
    variables:
      IP:
        description: "SonicWALL IP address or hostname"
        default: "192.168.168.168"
      PORT:
        description: "SonicWALL PORT"
        default: "443"

tags:
  - name: tfa
    description: Post user name, password and two-factor code to get bearer token.

  - name: auth
    description: logout current session.

  - name: config-pending
    description: "Pending configuraiton API."

  - name: administration
    description: "administration configuration API endpoint."
```

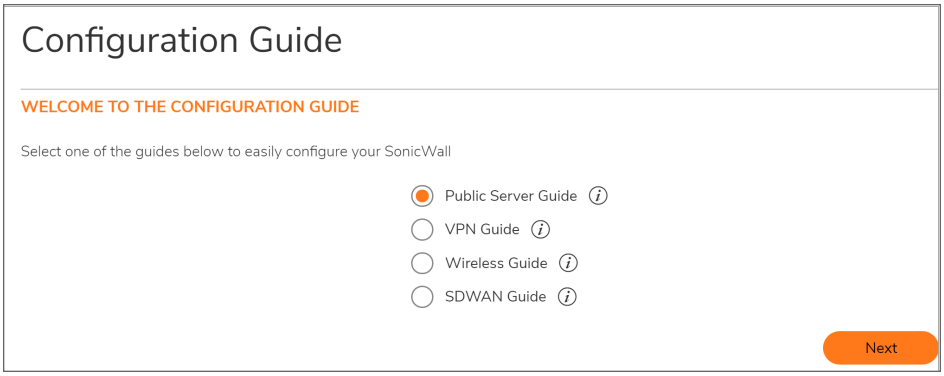
Legal Information

SonicWall SonicOS is protected by copyright and is provided *as is*.

The SonicWall copyright statement and End User Product Agreement (EUPA) are displayed on the **HOME | Legal Information** page.

SonicOS Guides (Wizards)

SonicOS provides easy-to-use configuration guides (wizards) to assist you with initial configuration of server access, VPN policies, wireless network and security settings, and Software-Defined WAN network settings.



Each wizard displays a sequence of screens in which you select or enter the necessary settings. To continue to the next screen, click **Next**. To go back and make a change, click **Previous**. To exit the wizard, click the **X**.

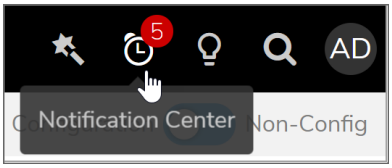
The **Summary** page displays all the objects, NAT policies, access rules, security settings, or other settings that will be created. To proceed, click **Apply**.

These configuration guides are available:

- Public Server Guide
- VPN Guide
- Wireless Guide
- SDWAN Guide

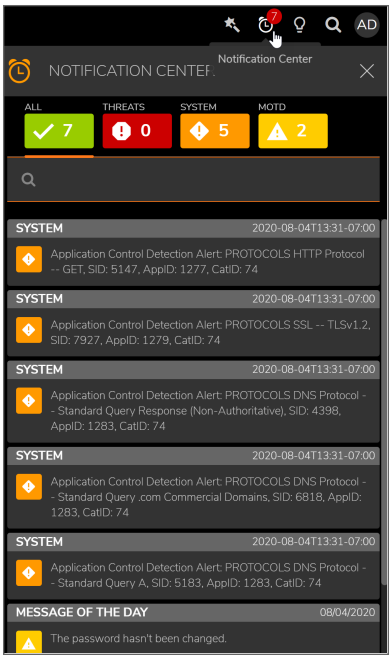
Notification Center

The SonicOS Notification Center provides actionable alerts with outstanding tasks to help administrators maintain their organization's security posture. The Notification Center is accessed by clicking the alarm clock button at the top right corner in the banner.



The number of current notifications is displayed in the red circle over the button.

The Notification Center displays a list of categorized messages with colored buttons at the top showing the number of each type.

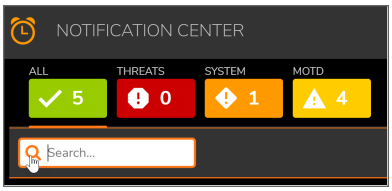


The notification categories are:

- **All** (Shows the total number of notifications)
- **Threats**
- **System**
- **MOTD** (Message of the Day)

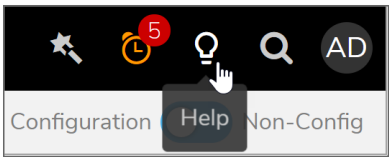
Click a category button to display notifications of that type only.

You can search the messages by clicking the Search icon and entering the value to search for into the field.



Online Help

Click the lightbulb icon at the top right in the banner to access SonicOS online help.



Your browser opens the SonicWall technical documentation page for your appliance platform and firmware version in another tab or window. From here, you can search for a keyword or open the relevant document.

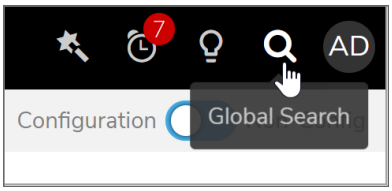
There are many administration guides for SonicOS, each covering a menu group such as **Dashboard** or **Rules and Policies**. For more information and a mapping of the SonicOS menu groups to the associated admin guides, refer to:

- Where Do I Find Information About SonicOS?
- SonicOS Web Interface to Admin Guides Reference

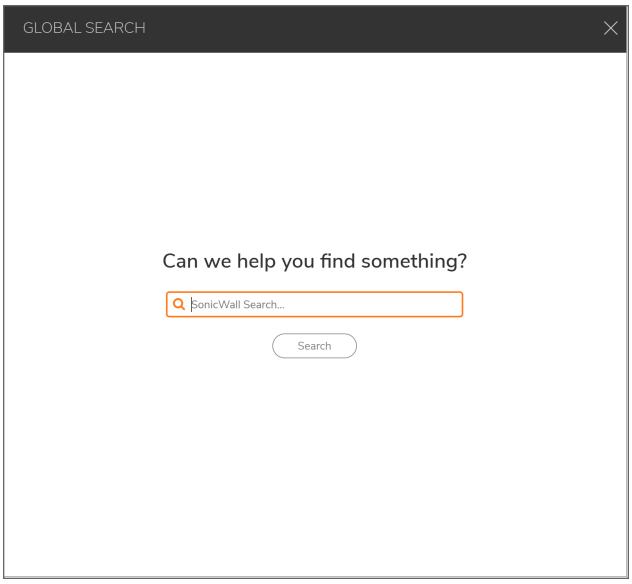
Global Search

SonicOS provides a global search feature that lets you look up elements in the web management interface, including page names, options, fields and so forth in the user interface itself, as well as configured values within features. This option to search for parameters globally helps the administrator to determine the sections, such as within Objects or Policies, in which the parameters are referenced.

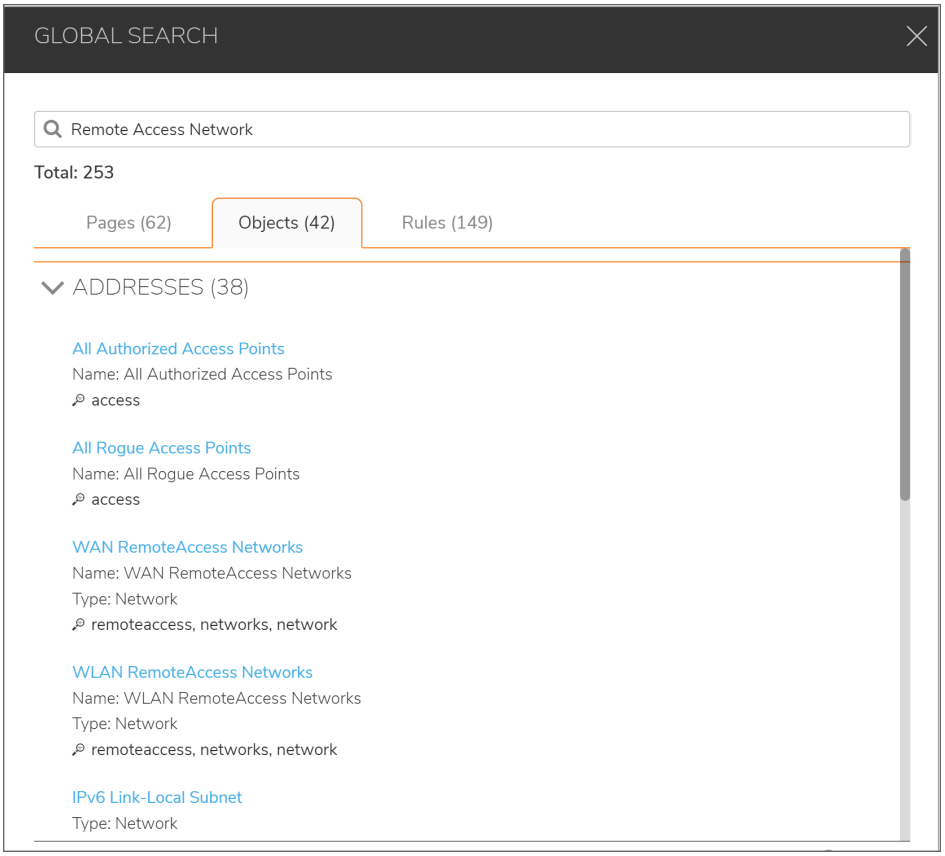
Launch a search by clicking the Global Search button at the top right, in the banner.



In the Global Search dialog, type in the string to search.



The results are displayed in the dialog, and may be divided by category. The number of results in each category is displayed in the category tab. Below, the categories are **Pages**, **Objects**, and **Rules**.



Click on any result to go to that location.

3

SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

About SonicOS
Updated - October 2024
Software Version - 8
232-006176-00 Rev A

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

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

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