Preface

Organization of this Guide

The SonicOS 6.2 Administration Guide is structured into the following parts that follow the SonicOS Management Interface structure. Within these parts, individual chapters correspond to the SonicOS management interface (UI) layout.

Topics:
- Part 1 Introduction
- Part 2 Dashboard
- Part 3 System
- Part 4 Network
- Part 5 Switching
- Part 6 3G/4G/Modem
- Part 7 Wireless
- Part 8 SonicPoint
- Part 9 Firewall
- Part 10 Firewall Settings
- Part 11 DPI-SSL
- Part 12 DPI-SSH
- Part 13 Capture ATP
- Part 14 VoIP
- Part 15 Anti-Spam
- Part 16 VPN
- Part 17 SSL VPN
- Part 18 Virtual Assist
- Part 19 User Management
- Part 20 High Availability
- Part 21 Security Services
- Part 22 WAN Acceleration
- Part 23 AppFlow
- Part 24 Log
- Part 25 Wizards (Guides)
- Part 26 Appendices

Part 1 Introduction

This part provides an overview of new SonicOS features, guide conventions, support information, and an overview of the SonicOS management interface.

The Introduction part contains the:
- Preface – Provides information about the guide itself, conventions, and support information.
- Introduction – Provides an overview of the SonicOS management interface.

Part 2 Dashboard

The Visualization Dashboard offers an effective and efficient interface to visually monitor your network in real time, providing effective flow charts of real-time data, customizable rules, and flexible interface settings.

NOTE: App Visualization (Real-Time Monitor and AppFlow Monitor) is supported on TZ series and above appliances.

The Dashboard part describes these UI pages:
- Multi-Core Monitor—Displays dynamically updated statistics on utilization of the individual cores of the SonicWall Security Appliance.

NOTE: Real-Time Monitor is supported on TZ series and above appliances.
- AppFlow Dash—Provides the same information that is provided in Dashboard > AppFlow Reports. Only in AppFlow Dash, the information is shown in graphs for the top one through ten items in each category.
- AppFlow Monitor—Provides real-time, incoming and outgoing network data. Various views and customizable options in the AppFlow Monitor Interface assist in visualizing the traffic data by applications, users, URLs, initiators, responders, threats, VoIP, VPN, devices, or by contents.
- AppFlow Reports—Provides configurable scheduled reports by applications, viruses, intrusions, spyware, and URL rating. AppFlow Reports

Part 1 Introduction

This part provides an overview of new SonicOS features, guide conventions, support information, and an overview of the SonicOS management interface.

The Introduction part contains the:
- Preface – Provides information about the guide itself, conventions, and support information.
- Introduction – Provides an overview of the SonicOS management interface.

Part 2 Dashboard

The Visualization Dashboard offers an effective and efficient interface to visually monitor your network in real time, providing effective flow charts of real-time data, customizable rules, and flexible interface settings.

NOTE: App Visualization (Real-Time Monitor and AppFlow Monitor) is supported on TZ series and above appliances.

The Dashboard part describes these UI pages:
- Multi-Core Monitor—Displays dynamically updated statistics on utilization of the individual cores of the SonicWall Security Appliance.

NOTE: Real-Time Monitor is supported on TZ series and above appliances.
- AppFlow Dash—Provides the same information that is provided in Dashboard > AppFlow Reports. Only in AppFlow Dash, the information is shown in graphs for the top one through ten items in each category.
- AppFlow Monitor—Provides real-time, incoming and outgoing network data. Various views and customizable options in the AppFlow Monitor Interface assist in visualizing the traffic data by applications, users, URLs, initiators, responders, threats, VoIP, VPN, devices, or by contents.
- AppFlow Reports—Provides configurable scheduled reports by applications, viruses, intrusions, spyware, and URL rating. AppFlow Reports
statistics enable you to view a top-level aggregate report of what is going on in your network.

- **Threat Reports**—Provides reports of the latest threat protection data from a single SonicWall appliance and aggregated threat protection data from SonicWall Security Appliances deployed globally.
- **User Monitor**—Displays details on all user connections to the SonicWall Security Appliance.
- **BWM Monitor**—Displays per-interface bandwidth management for ingress and egress network traffic. The BWM Monitor graphs are available for real-time, highest, high, medium high, medium, medium low, low and lowest policy settings.
- **Connection Monitor**—Displays details on all active connections to the SonicWall Security Appliance.
- **Packet Monitor**—Allows you to monitor individual data packets that traverse your firewall. Packets can be either monitored or mirrored. The monitored packets contain both data and addressing information.
- **Log Monitor**—Provides event log tracking for potential security threats. The log is displayed in a table and can be sorted by column. The SonicWall Security Appliance can alert you of important events, such as an attack to the firewall.

**Part 3 System**

This part covers a variety firewall controls for managing system status information, registering the firewall, activating and managing licenses, configuring management options, managing firmware versions, and using diagnostics tools for troubleshooting.

The System part describes these UI pages:

- **Status**—Provides system information such as firmware version and system up time, security services license status, per firewall blade alert messages, and network interface zone assignments and link status.
- **Licenses**—Describes how to activate, upgrade, or renew SonicWall Security Services licenses. From this page, you can manage all the SonicWall Security Services licensed for your SonicWall Security Appliance.
- **Administration**—Provides settings for the configuration of the SonicWall Security Appliance for secure and remote management. You can manage the firewall using a variety of methods, including HTTPS or SonicWall GMS.
- **SNMP**—Provides settings for the configuration of Simple Network Management Protocol (SNMP) for the management of IP networks.
- **Certificates**—Describes how to implement the use of certificates for VPN policies and how to locate sources for valid CA certificates from third party CA services.
- **Time**—Describes how to define the time and date settings for time stamp log events, how to automatically update security services, and how to use time and date for other internal purposes.
- **Schedules**—Describes how to create and manage objects for enforcing schedule times for a variety of firewall features.
- **Settings**—Describes how to manage your firewall’s SonicOS versions and preferences.
- **Packet Monitor**—Describes how to monitor individual data packets that traverse the firewall. The packet monitor feature provides the functionality to examine network traffic without the use of external utilities.
- **Diagnose**—Provides several diagnostic tools which help troubleshoot network problems as well as Active Connections, CPU, and Process Monitors.
- **Restart**—Provides instructions on how to restart the firewall from the Web Management interface.
- **Legal Information**—Provides easy access to the SonicWall End User Product Agreement.

**Part 4 Network**

This part covers configuring the SonicWall Security Appliance for your network environment.

The Network part describes these UI pages:

- **Interfaces**—Configures logical interfaces for connectivity. Configure interface objects that are directly linked to physical interfaces. The SonicOS scheme of interface addressing works in conjunction with network zones and address objects.
- **PortShield Groups**—Enables you to configure some or all of the LAN ports into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. For TZ series appliances, also enables you to add and configure Dell X-Series switches.
- **VLAN Translation**—On all wire mode-capable devices, enables you allow map incoming VLAN traffic on a Wire Mode Interface operating in secure mode to a different, outgoing VLAN on a wire-mode pair.
- **Failover & LB**—Configures one of the user-defined interfaces to act as a secondary WAN port for backup or load balancing.
- **Zones**—Configures security zones on your network.
- **DNS**—Sets up DNS servers for name resolution.
- **Address Objects**—Configures host, network, and address objects. Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface.
- **Services**—Configures service objects to be used network access rules for allowing or denying traffic to the network. The SonicWall Security Appliance includes Default Services. Default Services are predefined services that are not editable. And you can also create Custom Services to configure firewall services to meet your specific business requirements.
- **Routing**—Displays the Route Table, ARP Cache and configures static and dynamic routing by interface.
- **NET Policies**—Creates NAT policies including One-to-One NAT, Many-to-One NAT, Many-to-Many NAT, or One-to-Many NAT.
- **ARP**—Displays the ARP settings and clears the ARP cache as well as configure ARP cache time.
- **Neighbor Discovery**—Configures Neighbor Discovery Protocol (NDP) (IPv6 only).
- **MAC-IP Anti-spoof**—Configures MAC-IP Anti-Spoof protection in SonicOS.
- **DHCP Server**—Configures the firewall as a DHCP Server on your network to dynamically assign IP addresses to computers on your LAN or DMZ zones.
- **IP Helper**—Configures the firewall to forward DHCP requests originating from the interfaces on the firewall to a centralized server on behalf of the requesting client.
- **Web Proxy**—Configures the firewall to automatically forward all Web proxy requests to a network proxy server.
- **Dynamic DNS**—Configures the firewall to dynamically register its WAN IP address with a DDNS service provider.
- **Network Monitor**—Monitors network path viability, dynamically displays the results and status of this monitoring, provides the data to affected client components and logs it in the system log. Each custom Network Monitor policy defines a destination Address Object to be probed. This Address Object may be a Host, Group, Range, or FQDN. When the destination Address Object is a Group, Range or FQDN with multiple resolved addresses, Network Monitor probes each probe target and derives the Network Monitor Policy state based on the results.
Part 5 Switching

NOTE: Advanced switching and Link Aggregation are supported on NSA 3600 and higher appliances. The NSA 2600 supports Link Aggregation for Network Interfaces, but does not support Switching and, therefore, does not support Link Aggregation for Switching.

This part describes how to configure and manage the Switching feature of SonicOS on SuperMassive appliances and NSA appliances (except the NSA 2600).

The Switching part describes these UI pages:

- VLAN Trunking – Provides the ability to trunk different VLANs between multiple switches.
- Layer 2 Network Discovery – Uses IEEE 802.1AB (LLDP) and Microsoft LLTD protocols and switch forwarding table to discover devices visible from a port.
- Link Aggregation – Provides the ability to aggregate ports for increased performance and redundancy.
- Port Mirroring – Allows you to assign a mirror port to mirror ingress, egress or bidirectional packets coming from a group of ports.

Part 6 3G/4G/Modem

This part covers the status and configuration of SonicWall network Security Appliances with a USB extension port that support either an external 3G/4G interface or analog modem interface.

The 3G/4G/Modem part describes these UI pages:

- Status — Displays the status of the 3G/4G/modern appliance.
- Settings — Configures the firewall to automatically forward all Web proxy requests to a network proxy server.
- Advanced — Configures features such as remotely triggered dial-out, bandwidth management, and connection limit.
- Connection Profiles — Sets a host/node limit on the 3G/4G connection. This feature is especially useful for deployments where the 3G/4G connection is used as an overflow or in load-balanced situations to avoid over-taxing the connection.
- Data Usage — Monitors and displays the amount of data transferred over the 3G/4G interface.

Part 7 Wireless

This part covers the configuration of the built-in 802.11 radios for wireless SonicWall network security appliances.

The Wireless part describes these UI pages:

- Status — Provides status information for the wireless network: WLAN settings, WLAN statistics, WLAN activities, and station status.
- Settings — Configures settings for the 802.11 wireless antenna.
- Security — Configures the encryption mode for authentication.
- Advanced — Specifies advanced settings, such as radio settings.
- MAC Filter List — Creates lists of allowed and/or denied groups.
- IDS — Schedules Wireless Intrusion Detection Services (IDS), enables rouge access point detection, and displays discovered access points.
- Virtual Access Point — Configures Virtual Access Point (VAP) groups, VAPs, and VAP profiles.

Part 8 SonicPoint

SonicWall SonicPoints are wireless access points specially engineered to work with SonicWall Security Appliances to provide wireless access throughout an enterprise.

The SonicPoint part describes these UI pages:

- SonicPoints—Describes how to use SonicPoints (wireless access points) with SonicWall Security Appliances to provide wireless access throughout your enterprise, and how to manage the SonicPoints connected to your system.
- Station Status—Displays reports on the statistics of each SonicPoint.
- IDS—Displays reports on all access points that can be found by scanning the 2.4GHz and 5GHz radio bands on the SonicPoints.
- Advanced IDP—Monitors the radio spectrum for presence of unauthorized access points (intrusion detection) and to take countermeasures automatically (intrusion prevention) according to your settings.
- Virtual Access Point—Allows multiple virtual access points to exist within a single physical access point.
- RF Monitoring—Provides real-time monitoring of RF traffic for threats, and provides information to help best utilize the wireless bandwidth with SonicPoints.
- RF Analysis—Describes how to use the RF Analysis feature to best utilize the wireless bandwidth with SonicPoint and SonicPoint-N appliances.
- FairNet—Provides an easy-to-use method for you to control the bandwidth of associated wireless clients and make sure it is distributed fairly between them. You can configure the SonicPoint FairNet bandwidth limits for all wireless clients, specific IP address ranges, or individual clients to provide fairness and network efficiency.
- Wi-Fi Multimedia—Provides support for Wi-Fi Multimedia (WMM) on bandwidth-intensive applications such as VoIP, VoIP on Wi-Fi phones, and multimedia traffic on wireless IEEE 802.11 networks.

Part 9 Firewall

This part describes Access Rules and App Rules, which are application-specific policies that give you granular control over network traffic on the level of users, email users, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, Email, and Email attachments.

The Firewall part describes these UI pages:
Part 10 Firewall Settings

This part describes the tools for managing how the SonicWall Security Appliance handles traffic through the firewall.

The Firewall Settings part describes these UI pages:

• Advanced – Provides advanced firewall settings for configuring detection prevention, dynamic ports, source routed packets, connection selection, and access rule options.
• BWM – Provides a means of allocating bandwidth resources to critical applications on a network.
• Flood Protection – Displays statistics on TCP Traffic through the Security Appliance and manages TCP traffic settings.
• Multicast – Configures IP multicasting, a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic — multimedia presentations and video conferencing.
• QoS Mapping – Provides a method to manage Quality of Service (QoS), a diversity of methods intended to provide predictable network behavior and performance.
• SSL Control – Describes how to plan, design, implement, and maintain the SSL Control feature.

Part 11 DPI-SSL

This part describes the Deep Packet Inspection Secure Socket Layer (DPI-SSL) feature to allow for the inspection of encrypted HTTPS traffic and other SSL-based traffic. DPI-SSL is supported on all appliance platforms.

The DPI-SSL part describes these UI pages:

• Client SSL — Inspects HTTPS traffic when clients on the SonicWall Security Appliance’s LAN access content located on the WAN.
• Server SSL — Inspects HTTPS traffic when remote clients connect over the WAN to access content located on the SonicWall Security Appliance’s LAN.

Part 12 DPI-SSH

This part describes the Deep Packet Inspection Secure Shell (DPI-SSH) feature to allow for the secure remote communication between two networked computers.

The DPI-SSH part describes these UI pages:

• Configure – Enables various SSH inspection and configures exclusion and inclusion address objects/groups, service objects/groups, and/or user objects and groups.

Part 13 Capture ATP

This part describes the Capture Advanced Threat Protection (ATP) feature that provides analysis of files for malicious elements such as malware or viruses.

The Capture ATP part describes these UI pages:

• Status – Provides graphical and log analysis threats encountered in files.
• Settings – Configures Capture ATP settings.

Part 14 VoIP

This part provides instructions for configuring the SonicWall Security Appliance to support H.323 or SIP Voice over IP (VoIP) connections.

The VoIP part describes these UI pages:

• Settings – Configures VOIP settings, including SIP and H.325 settings.
• Call Status – Provides a listing of currently active VoIP calls

Part 15 Anti-Spam
NOTE: Anti-Spam is available on all platforms except SuperMassive appliances.

This part provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing firewall.

The Anti-Spam part describes these UI pages:

- Status – Displays the state of licensing and monitoring and provides email diagnostics.
- Settings – Sets Anti-Spam preferences, installs the SonicWall Junk Store, and configures email threat categories.
- Statistics – Displays the statistics on how many messages are being blocked by the Anti-Spam for the appliance feature.
- RBL Filter – This is the same as the Security Services > RBL Filter page and is described in that chapter.
- Junk Box Summary – Displays the number of blocked messages (per user) and a list of quarantined emails, with corresponding links to view and unjunk these messages.
- Junk Box View – Displays view and manages all email messages that are currently in the Junk Store on the Exchange or SMTP server.
- Junk Box Settings – Sets the length of time that messages are stored in the Junk Box before being deleted and the number of Junk Box messages to be displayed per page.
- User View Setup – Configures which settings will be visible for users.
- Address Books – Specifies Allowed and Blocked lists.
- Manage Users – Adds, removes, and manages all users, on both the Global and LDAP servers.
- LDAP Configuration – Configures various settings specific to the LDAP server.
- Advanced – Downloads system or log files, as well as configures the log level.
- Downloads – Downloads and installs one of SonicWall’s latest spam-blocking buttons.

Part 16 VPN

This part covers how to create VPN policies on the SonicWall Security Appliance to support Global VPN Clients as well as creating site-to-site VPN policies for connecting offices running SonicWall Security Appliances.

The VPN part describes these UI pages:

- Settings – Provides the features for configuring VPN policies, both site-to-site VPN policies and GroupVPN policies.
- Advanced – Configure settings that globally affect all VPN policies, and provides solutions for Online Certificate Status Protocol (OCSP).
- DHCP over VPN – Configures a firewall to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space, which facilitates IP address administration for networks using VPN tunnels.
- L2TP Server – Provides secure access to resources behind the firewall.

Part 17 SSL VPN

This part describes how to configure the SSL VPN features on the SonicWall Security Appliance. SSL VPN features provide secure, seamless, remote access to resources on your local network using the NetExtender client.

The SSL VPN part describes these UI pages:

- Status – Displays a summary of active NetExtender sessions, including the name, the PPP IP address, the physical IP address, login time, length of time logged in and logout time.
- Server Settings – Configures details of the firewall’s behavior as an SSL VPN server.
- Client Settings – Enable SSL VPN access on zones and configures the client address range information and NetExtender client settings. It also displays which zones have SSL VPN access enabled.
- Portal Settings – Configures the appearance and functionality of the SSL VPN Virtual Office web portal. The Virtual Office portal is the website that uses log in to launch NetExtender. It can be customized to match any existing company website or design style.
- Virtual Office – Displays the Virtual Office web portal inside of the SonicOS UI.

Part 18 Virtual Assist

This part describes the Virtual Assist feature, which allows you to support customer technical issues without having to be on-site with the customer. This capability serves as an immense time-saver for support personnel, while adding flexibility in how they can respond to support needs. You can allow or invite customers to join a “queue” to receive support, then virtually assist each customer by remotely taking control of a customer’s computer to diagnose and remedy technical issues.

The Virtual Assist part describes these UI pages:

- Status – Allows customers to log in to receive technical support by adding their names to a queue.
- Settings – Configures settings within the SonicOS management interface, such as notification settings, request settings, and restriction settings.

Part 19 User Management

This part covers how to configure the SonicWall Security Appliance for user-level authentication as well as manage guest services.

The Users part describes these UI pages:

- Status – Displays the Active User Sessions on the firewall.
- Settings – Configures the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto the network.
- Local Users – Displays and manages all local users, adds new local users, edits existing local users, and imports users from the LDAP server.
- Local Groups – Configures local user groups in SonicOS by retrieving the user group names from the LDAP server and provides the ability to set LDAP rules and policies for users located in certain Organizational Units (OUs) on the LDAP server.
• Guest Services – Sets up guest accounts, temporary accounts set up for users to log into your network, and determine the limits and configuration of the guest accounts.
• Guest Accounts – Displays the guest services accounts on the Security Appliance.
• Guest Status – Reports on all the guest accounts currently logged in to the Security Appliance.

Part 20 High Availability

**NOTE:** High Availability is supported on TZ series and above appliances. Active/Active Clustering is supported on NSA 2600 and above appliances.

This part explains how to configure the SonicWall Security Appliance for high availability so that in case of a loss of network connectivity, another SonicWall Security Appliance resumes all active connections.

The High Availability part describes these UI pages:

• Status – Displays the current status of the HA Pair, HA configuration, and HA licenses.
• Settings – Configures the HA settings.
• Advanced – Provides the ability to fine-tune the High Availability configuration as well as synchronize setting and firmware among the High Availability devices.
• Monitoring – Configures independent management IP addresses for each unit in the HA Pair, using either LAN or WAN interfaces and configures physical/link monitoring and logical/probe monitoring.

Part 21 Security Services

This part includes an overview of available SonicWall Security Services as well as instructions for activating the service, including FREE trials. These subscription-based services include SonicWall Gateway Anti-Virus, SonicWall Intrusion Prevention Service, SonicWall Content Filtering Service, SonicWall Client Anti-Virus.

The Security Services part describes these UI pages:

• Summary – Lists the security services that are available, with a short description of the service, and allows for global configuration of security services licensing as well as management of signatures and security service settings.
• Content Filter – Configures the Restrict Web Features and Trusted Domains settings, which are included with SonicOS, activates and configures the SonicWall Content Filtering Service (SonicWall CFS) as well as a third-party Content Filtering product.
• Client AV Enforcement – Configures Client Anti-Virus policies and enforcement.
• Client CF Enforcement – Enables and configures settings for Client CF enforcement and management.
• Gateway Anti-Virus – Configures Gateway Anti-Virus Service to enforce anti-virus policies at the gateway to ensure all users have the latest updates and monitor files as they come into the network.
• Intrusion Prevention – Displays the Intrusion Prevention Service (IPS) status and configures IPS global settings and policies.
• Anti-Spyware – Configures settings for managing the service on a SonicWall Security Appliance.
• RBL Filter – Configures SMTP Real-Time Black List (RBL), a mechanism for publishing the IP addresses of SMTP spammers use.

**NOTE:** The Security Services > RBL Filter page is the same as the Anti-Spam > RBL Filter page on platforms that support Anti-Spam. Anti-Spam is not supported in SuperMassive 9000 series.

• Geo-IP Filter – Configures the Geo-IP Filter feature, which blocks connections to or from a geographic location. The SonicWall network Security Appliance uses IP address to determine to the location of the connection. This page also customizes a web-blocked page, displays Geo IP cache statistics, and performs Geo location server lookup.

**NOTE:** Geo-IP filtering and Botnet Filtering are supported on TZ series and above appliances.

• Botnet Filter – Configures the Botnet Filter feature, which blocks connections to or from Botnet command and control servers, customizes a web-blocked page, displays Botnet cache statistics, and performs Botnet server lookup.

Part 22 WAN Acceleration

This part provides an overview of the SonicWall WXA series appliance, basic and advanced deployment scenarios, and configuration and verification examples.

The WAN Acceleration part describes these UI pages:

• Summary – Provides a dashboard view of the System Information, TCP Acceleration, WFS Acceleration, and Web Cache of a SonicWall WXA series appliance.
• TCP Acceleration – Configures and monitors the TCP Acceleration service.
• WFS Acceleration – Configures and monitors the WFS Acceleration service.
• Web Cache – Configures and monitors the Web Cache service.
• System – Configures and monitors the System Status, Interface Status, Management, Settings, and Firmware tabs.
• Logs – Displays a detailed list of the SonicWall WXA series appliance’s log event messages.

Part 23 AppFlow

**NOTE:** The AppFlow feature is available on TZ series and above appliances.

This part covers managing the SonicWall Security Appliance’s flow reporting statistics and configurable settings for sending AppFlow and real-time data to local or external collector servers. The SonicWall Security Appliance AppFlow provides support for external AppFlow reporting formats, such as NetFlow version 5, NetFlow version 9, IPFIX with extensions, and Quest™ Change Auditor for SonicWall.
The AppFlow part describes these UI pages:

- **Flow Reporting** – Displays statistics based on Flow Reporting and Internal Reporting and configures settings for internal reporting and AppFlow server reporting.
- **GMSFlow Server** – Establishes a connection to a GMSFlow Server.
- **Real-Time Monitor** – This is the same as the Dashboard > Real-Time Monitor page and is described in that chapter.
- **AppFlow Server** – Configures a SonicWall AppFlow Server as an external collector for AppFlow and real-time data reporting and analysis.
- **AppFlow Dash** – This is the same as the Dashboard > AppFlow Dash page and is described in that chapter.
- **Appflow Monitor** – This is the same as the Dashboard > AppFlow Monitor page and is described in that chapter.
- **Appflow Reports** – This is the same as the Dashboard > AppFlow Reports page and is described in that chapter.

**Part 24 Log**

This part covers managing the SonicWall Security Appliance’s enhanced logging, alerting, and reporting features. The SonicWall Security Appliance’s logging features provide a comprehensive set of log categories for monitoring security and network activities.

The Log part describes these UI pages:

- **Log Monitor** – This is the same as the Dashboard > Log Monitor page and is described in that chapter.
- **Settings** – Categorizes and customizes the logging functions on a SonicWall Security Appliance for troubleshooting and diagnostics.
- **Syslog** – Captures all log activity and displays every connection source and destination IP address, IP service, and number of bytes transferred.
- **Automation** – Configures the SonicWall to send log files using email and configures mail server settings.
- **Name Resolution** – Configures the name servers used to resolve IP addresses and server names in the log reports.
- **Reports** – Displays a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth.
- **Analyzer** – Adds the IP address and port number of an Analyzer server.

**Part 25 Wizards (Guides)**

This part describes how to use the configuration wizards, called Guides, for configuring SonicWall appliances.

- **Setup Guide** – Steps through network configuration for Internet connectivity.
  
  **NOTE:** The TZ series and SOHO Wireless appliances have an initial Setup Guide that displays when you first start up the appliance.
- **PortShield Interface Guide** — Steps through selecting the initial ports assignment in integrated managed LAN switch of the SonicWall Security appliance.
- **Public Server Guide** – Steps through adding a server to your network, such as a mail server or a Web server.
- **VPN Guide** – Steps through the configuration of Group VPNs and site-to-site VPNs.
- **WXA Setup Guide** — Steps through configuring the coupled WXA series appliance for WAN Acceleration.

**Part 26 Appendices**

**Appendix A: OAuth, Social Login, and LHM**

This appendix describes SonicWall’s implementation of the Open Authentication (OAuth) Social Login feature and Lightweight Hotspot Messaging (LHM) feature as well as how to configure SonicOS to work with social networking services such as Facebook, Twitter, or Google+.

**Appendix B: BGP**

This appendix describes of SonicWall’s implementation of Border Gateway protocol (BGP), how BGP operates, and how to configure BGP for your network.

**Appendix C: IPv6**

This appendix describes the SonicOS implementation of IPv6, how IPv6 operates, and how to configure IPv6 for your network.

**Appendix D: VPN Auto Provisioning**

This appendix describes the VPN Auto Provisioning feature, which simplifies the provisioning of site-to-site VPNs between two SonicWall firewalls.

**Appendix E: SonicWall Support**

This appendix contains information about using the SonicWall Support Portal for documentation and self-help tools as well as how to contact SonicWall Tech Support.

**Conventions**

**Text Conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>Highlights items you can select in the SonicOS management</td>
</tr>
</tbody>
</table>
About SonicOS

The web-based SonicOS management interface allows you to configure and administer SonicWall network security appliances (firewalls) running SonicOS 6.2:

- SuperMassive 9800
- NSA 6600
- TZ600
- SOHO Wireless
- SuperMassive 9600
- NSA 5600
- TZ300/TZ500 Wireless
- SuperMassive 9400
- NSA 4600
- TZ400/TZ400 Wireless
- SuperMassive 9200
- NSA 3600
- TZ300/TZ300 Wireless
- NSA 2600

Management Interface

SonicOS provides an easy-to-use, graphical interface for configuring your network security appliance. The following sections provide an overview of the key management interface features:

- Dynamic User Interface
- Navigating the Management Interface
- Icons and Buttons in the Management Interface
- Status bar
- Applying Changes
- Tooltips
- Navigating Dynamic Tables
- Management Interface Options
- Command Line Interface (CLI)
- Registering Your SonicWall Security Appliance

Dynamic User Interface

Table statistics and log entries are dynamically updated within the user interface without requiring users to reload their browsers. 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 firewall.
Navigating the Management Interface

Navigating the management interface is facilitated by a hierarchy of menu items on the navigation bar (left side of your browser window). When you click a menu item, related management functions are displayed as submenu items in the navigation bar.

If the navigation bar continues below the bottom of your browser, up-and-down arrow buttons appear in the bottom right corner of the navigation bar. Mouse over the up or down arrow to scroll the navigation bar up or down. You also can use the scroll wheel on your mouse.

Icons and Buttons in the Management Interface

Topics:
- Common Icons
- Display Icons
- Common Buttons

Common 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. Common icons describes the functions of common icons used in the Management Interface:

<table>
<thead>
<tr>
<th>Action</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit</td>
<td>📝</td>
<td>Displays a dialog (secondary or popup window) for editing the settings.</td>
</tr>
<tr>
<td>Delete</td>
<td>🗑️</td>
<td>Deletes a table entry.</td>
</tr>
<tr>
<td>Comment</td>
<td>📜️</td>
<td>Displays text from a field entry or information about the table entry.</td>
</tr>
<tr>
<td>Funnel</td>
<td>🤔</td>
<td>Indicates access rules with bandwidth management.</td>
</tr>
<tr>
<td>Upload</td>
<td>⌨️</td>
<td>Uploads a file to a common database or external switch.</td>
</tr>
<tr>
<td>Print</td>
<td>📄</td>
<td>Exports the data flow to a printer or file.</td>
</tr>
<tr>
<td>Print PDF</td>
<td>📃</td>
<td>For some UI pages, prints a pdf file.</td>
</tr>
<tr>
<td>Report</td>
<td>📊</td>
<td>Downloads a visualization report.</td>
</tr>
<tr>
<td>Send Report</td>
<td>📡</td>
<td>Sends the log to an email address.</td>
</tr>
<tr>
<td>Refresh</td>
<td>🔄</td>
<td>Updates the real-time data in a table, chart, or other display.</td>
</tr>
<tr>
<td>Notes</td>
<td>📖</td>
<td>Displays a popup balloon containing status or statistics about an entry in tables.</td>
</tr>
<tr>
<td>Statistics</td>
<td>📈</td>
<td>Displays a popup balloon containing statistics about an entry in tables or general status about the table or page.</td>
</tr>
</tbody>
</table>
Clear
Statistics
Updates the statistics shown in the traffic tables.

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.

Left-arrow
Displays a pop-up balloon containing the respective VPN policy in the middle of the page.

Priority
Displays a pop-up containing statistics about an entry in tables or general status about the table or page.

Enabled
Indicates the interface or service is enabled. Clicking on the icon disables the interface or service.

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.

Solid indicates that all members of the category, group, or event are enabled.

Semi-solid indicates that some are enabled, some are disabled.

Disabled
Indicates the interface or service is disabled. 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.

Link
Provides a link to another page in the UI. Clicking the link displays the page.

Import
Imports certificate information or images.

Reboots the firewall with the firmware version listed in the same row.

Export
Exports a 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.

Exports the log as a CSV-format file. Clicking this icon displays a dialog that allows you to open or save the log in CSV format.

Exports the log as a plain text-format (.txt) file.

Boot
Imports certificate information or images.

Reboots the firewall with the firmware version listed in the same row.

Information
Displays popup dialogs containing more detailed information than displayed on the page.

Question
Mark
Help
Displays information about an option or setting on a page, report, or dialog; see Tooltips.

Search
Searches a table for the specified data.

NOTE: The Search icon and the Search button are used on different pages.

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.

Collapse
Hides a chart, table, or section of a management interface page to allow more display room for other data.

Expand
Redisplays a hidden chart, table, or section of a management interface page.

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 Icons.
Pause

Freezes the data flow. The time and date also freeze.

The Pause icon appears gray 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, and when clicked, the 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 gray 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, and when clicked, the Play icon becomes the Pause icon.

Stop

Stops services for an appliance.

Start

Resumes stopped services for an appliance.

Reject

Disables a built-in common name, but does not delete it.

Accept

Enables a built-in common name.

Add

Displays a dialog (secondary or popup window) for adding entries to a table.

Remove

Removes a local user from a group.

Clock

Displays a popup balloon containing information about account and session expirations.

Displays a popup balloon containing information about schedules.

Chart

Format:

Toggles the display of a chart between bar and flow (area) formats.

Bar Chart

Flow (Area)

Chart

NetExtender

Launches and configures NetExtender.

Display Icons

Most submenus in the Dashboard menu have a Display icon associated with them. Clicking on the icon for a submenu item opens a new tab in your browser that displays only the report or graph associated with that submenu item. You can display all these submenu items or only the ones of interest. When the submenu item is in a new tab, you can move the tab to a new browser window to display separately from the management interface.

Other submenus that display sometimes rapidly changing data also have a Display icon associated with them. This icon is located at the top of the submenu page near the Mode option. This Display icon works the same as those of the Dashboard submenus and is also associated with them.

Common 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. Common buttons describes the functions of common buttons used in the management interface:

<table>
<thead>
<tr>
<th>Action</th>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td><img src="accept.png" alt="Accept" /></td>
<td>Applies the changes entered on certain Interface Management pages.</td>
</tr>
<tr>
<td>OK</td>
<td><img src="ok.png" alt="OK" /></td>
<td>Applies the changes entered on the Interface Management page or for a dialog, applies the changes and closes the dialog.</td>
</tr>
<tr>
<td>Save</td>
<td><img src="save.png" alt="Save" /></td>
<td>Applies the changes made in a dialog and then closes the dialog.</td>
</tr>
<tr>
<td>Apply</td>
<td><img src="apply.png" alt="Apply" /></td>
<td>Applies the changes made in a dialog, but does not close the dialog.</td>
</tr>
<tr>
<td>Cancel</td>
<td><img src="cancel.png" alt="Cancel" /></td>
<td>Discards the changes entered on the Interface Management page or for a dialog, discards any changes made in the dialog and closes the dialog.</td>
</tr>
<tr>
<td>Close</td>
<td><img src="close.png" alt="Close" /></td>
<td>Discards any changes made in the dialog and closes the dialog.</td>
</tr>
<tr>
<td>Help</td>
<td><img src="help.png" alt="Help" /></td>
<td>Displays the help page for the dialog.</td>
</tr>
<tr>
<td>Add</td>
<td><img src="add.png" alt="Add" /></td>
<td>Displays a dialog that allows you to add elements, such as zones, services, and access/firewall rules, to your appliance.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Configure</td>
<td>Displays a configuration dialog for configuring SonicOS settings.</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>Erases current values and restores factory default values.</td>
<td></td>
</tr>
<tr>
<td>Create Rule</td>
<td>Displays the dialog for creating AppFlow rules.</td>
<td></td>
</tr>
<tr>
<td>Refresh</td>
<td>Updates real-time data in a table.</td>
<td></td>
</tr>
<tr>
<td>Update</td>
<td>Updates entries in a table.</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected items from a table.</td>
<td></td>
</tr>
<tr>
<td>Delete Box</td>
<td>Deletes the item, especially in a filter.</td>
<td></td>
</tr>
<tr>
<td>Delete All</td>
<td>Deletes all items except default and system-generated items in a table.</td>
<td></td>
</tr>
<tr>
<td>Remove</td>
<td>Deletes the selected items from a table.</td>
<td></td>
</tr>
<tr>
<td>Remove All</td>
<td>Deletes all items in a table.</td>
<td></td>
</tr>
<tr>
<td>Flash</td>
<td>Removes one or more selected items in a table.</td>
<td></td>
</tr>
<tr>
<td>Flash All</td>
<td>Removes all items in a table.</td>
<td></td>
</tr>
<tr>
<td>Purge</td>
<td>Deletes one or more selected FQDN objects from a table.</td>
<td></td>
</tr>
<tr>
<td>Purge All</td>
<td>Deletes all FQDN objects from a table.</td>
<td></td>
</tr>
<tr>
<td>Clear</td>
<td>Clears the packet monitor queue and the displayed statistics for the capture buffer, mirroring, and FTP logging.</td>
<td></td>
</tr>
<tr>
<td>Clear Statistics</td>
<td>Clears the counters and the displayed statistics; restarts the counters.</td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>Correlates data among tabs in the AppFlow Monitor page.</td>
<td></td>
</tr>
<tr>
<td>Filter Add</td>
<td>Adds or deletes a filter based on selected criteria.</td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Installs a SonicWall SSO Agent feature.</td>
<td></td>
</tr>
<tr>
<td>Preview</td>
<td>Displays the HTML message in a dialog for verification of how the message looks.</td>
<td></td>
</tr>
<tr>
<td>Example Template</td>
<td>Reverts the HTML message code to the default HTML message.</td>
<td></td>
</tr>
<tr>
<td>Go</td>
<td>Performs the specified lookup.</td>
<td></td>
</tr>
<tr>
<td>Lookup</td>
<td>Performs the specified lookup.</td>
<td></td>
</tr>
<tr>
<td>Right Arrow</td>
<td>Moves an item from a generic list to a specific list.</td>
<td></td>
</tr>
<tr>
<td>Left Arrow</td>
<td>Removes an item from a specific list to a generic list.</td>
<td></td>
</tr>
<tr>
<td>Double Right Arrow</td>
<td>Moves items from a generic list to a specific list.</td>
<td></td>
</tr>
<tr>
<td>Double Left Arrow</td>
<td>Removes items from a specific list to a generic list.</td>
<td></td>
</tr>
</tbody>
</table>

**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 the Accept button at the top of the management interface 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 firewall 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 the Cancel button at the top of a management interface page or the bottom of a dialog.
ToolTips

Topics:
• Generic Tooltips
• Tooltips with Values
• Configuring Tooltips

Generic Tooltips

SonicOS provides embedded tooltips, or small pop-up 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 UI 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 appliance supports. For example, the Firewall > Address Objects page displays the maximum number of address groups the 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 can be configured in the Web Management Settings on the System > Administration page.

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

• Form Tooltips Delay - Duration in milliseconds before Tooltips display for forms (boxes where you enter text).
• Button Tooltips Delay - Duration in milliseconds before Tooltips display for radio buttons and checkboxes.
• Text Tooltips Delay - Duration in milliseconds before Tooltips display for UI text.

Manipulating Tables

Topics:
Navigating Dynamic Tables

In the SonicOS dynamic user 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:

A number of tables now include an option to specify the number of items displayed per page.

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. On some sortable tables, a Click to sort by tooltip appears when you mouse over the column headings.

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 Packets table is sorted by Priority.

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 one or more selected FQDN objects from a table, click the Purge button. To flush all the FQDN objects from the table, click the Purge All button.

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 tab on the Network > PortShield Groups page
- NAT Policies on the Network > NAT Policies page
- Relay Protocols on the Network > IP Helper page
- Access Rules on the Firewall > Access 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:

- Wizards (Guides)
- Help
- Logout
- Mode

**Wizards (Guides)**

NOTE: The terms wizards and guides are interchangeable.

Each firewall includes a Configuration Guide option that steps you through various firewall configurations, such as Setup, PortShield interface, Public Server, VPN policies, LAN network, wireless LAN network, and 3G/4G Modem. Clicking Wizards accesses the Configuration Guide dialog.

**Help**

Each firewall includes Web-based online help that explains how to use management interface pages and how to configure the firewall. 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 firewall.
- Non-Config mode – You can only view the settings of the firewall and cannot make any changes or view some management interface pages.

Clicking the arrow next to Mode: Configuration/Non-Config, allows you to toggle between configuration mode and non-configuration mode.

**Command Line Interface (CLI)**

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

**Registering Your SonicWall Security Appliance**

After you have established your Internet connection, it is recommended you register your SonicWall Security Appliance. Registering your SonicWall Security Appliance provides these benefits:

- Try a FREE 30-day trial of SonicWall Intrusion Prevention Service, SonicWall Gateway Anti-Virus, Content Filtering Service, and Client Anti-Virus
- Activate SonicWall Anti-Spam
- Activate SonicWall security services and upgrades
- Access SonicOS firmware updates
- Get SonicWall technical support

For instructions about creating a MySonicWall account as well as registering and licensing your SonicWall appliance, see the Getting Started Guide for your appliance and Managing SonicWall Licenses.

NOTE: Make sure the Time Zone and DNS settings on your appliance are correct when you register the device.

NOTE: mysonicwall.com registration information is not sold or shared with any other company.