SonicWall® SonicOS 6.5.4.3
Release Notes
May 2019

These release notes provide information about the SonicWall® SonicOS 6.5.4.3 release.

Topics:
• About SonicOS 6.5.4.3
• Supported Platforms
• New Hardware
• New Features
• Resolved Issues
• Known Issues
• System Compatibility
• Product Licensing
• Upgrading Information
• SonicWall Support

About SonicOS 6.5.4.3

SonicWall SonicOS 6.5.4.3 provides many new features and fixes a number of issues found in previous releases. This release introduces support for SonicWall’s new wireless access points, the SonicWave 200 series. For more information, see the New Hardware, New Features, and Resolved Issues sections.

This release supports all the features and contains all the resolved issues found in previous SonicOS 6.5 releases. For more information, see the previous release notes, available on MySonicWall at: https://mysonicwall.com.
Supported Platforms

SonicOS 6.5.4.3 is supported on the following SonicWall appliances:

- NSA 9650
- NSA 9450
- NSA 9250
- NSA 6650
- NSA 5650
- NSA 4650
- NSA 3650
- NSA 2650
- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600 / TZ600P
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ350 / TZ350 Wireless
- TZ300 / TZ300P / TZ300 Wireless
- SOHO 250 / SOHO 250 Wireless
- SOHO Wireless

New Hardware

SonicOS 6.5.4.3 supports the new SonicWave 200 series:

- **SonicWave 224w**
  The SonicWave 224w is a wall-mountable wireless access point suitable for indoor single-unit or multi-unit deployments. It is designed to connect to an Ethernet dual wall jack with one connection to a SonicWall firewall or other network device and a second, optional, connection to the same or another network device. You can power the SonicWave 224w with Power over Ethernet (PoE) or with a power adapter (both sold separately). The SonicWave 224w also has a 1GbE LAN port that provides PoE Out for an 802.3af device, such as an IP phone or IP camera. PoE Out is available when the SonicWave 224w is powered by PoE, but not when it is powered by the power adapter.

- **SonicWave 231c**
  The SonicWave 231c is a ceiling-mountable wireless access point suitable for indoor single-unit or multi-unit deployments. It is plenum rated for installation within an enclosed space such as an attic. It can also be mounted on a wall or deployed on a shelf, table, or desktop. You can power the SonicWave 231c with Power over Ethernet (PoE) or with a power adapter (both sold separately).

- **SonicWave 231o**
  The SonicWave 231o extends your wireless LAN past the traditional boundaries of indoor locations. With state of the art design and construction, it is resistant to harsh outdoor environments and extreme temperature changes. The unit is designed specifically for outdoor use. Waterproof connectors are supplied to ensure watertight seals for connecting the Ethernet cable to the device. The SonicWave 231o access point is suitable for outdoor single-unit or multi-unit deployments. Power over Ethernet (PoE) must be provided to power the SonicWave 231o.

All SonicWaves include dual 2.4GHz/5GHz radios with Dynamic Frequency Selection (DFS) providing wireless 802.11 b/g/n/ac (2x2 MIMO).

Secure Cloud Wireless for SonicWave Management

Both the SonicWave 200 series and the SonicWave 432 series can be managed by either a SonicWall firewall or by the new SonicWall Secure Cloud Wireless tools, including the SonicWiFi mobile app, WiFi Cloud Manager, and WiFi Planner. For more information about these, see the Secure Cloud Wireless for SonicWave Management and Secure Cloud Management of SonicWave Appliances sections in this document.

For complete information, point your browser to the SonicWall Technical Documentation portal at https://www.sonicwall.com/support/technical-documentation and select Secure Cloud Wireless in the Select A Product field.
New Features

This section describes the new features introduced in SonicOS 6.5.4.3.

Topics:

- DPI-SSL Connections Increased
- Globally Disable Unused Features
- Access Point Features
- CSC Flow Reporting and Visualization Support on SOHO W
- Expired Certificates Blocked in DPI-SSL Client
- Block Login Attempts by IP Address Range
- Enhanced Logging
- Increased IP Helper Policy Count
- Enhanced Cipher Control for SSL Communication

DPI-SSL Connections Increased

DPI-SSL connections have increased across platforms, and scale to support hundreds of thousands of connections, the number which is a function of the hardware platform.

Globally Disable Unused Features

Topics:

- One-Click Global Control of Wireless LAN and IPv6
- Disable VPN Policies

One-Click Global Control of Wireless LAN and IPv6

A new section, Feature Visibility, has been added to the MANAGE | System Setup > Base Settings page. This section contains two options that allow you to control the visibility of wireless LAN (WLAN) and/or IPv6:

- Enable Wireless LAN
- Enable IPv6
By selecting either or both of these options, you allow these features to be used, and they are visible on the MONITOR | Current Status > System Status page. If the options are not selected, the System Status page displays that they are disabled.

When WLAN is disabled:
- All access point and wireless-related management interface pages do not display.
- WLAN is not displayed as a zone type.
- Any existing WLAN zones or objects become uneditable.

When IPv6 is disabled, all IPv6 packets are dropped by the firewall and the INVESTIGATE | Tools > Packet Monitor page displays the log messages.

Disable VPN Policies
You can now disable default VPN policies and VPN-related configurations, such as Group VPN for WAN and WLAN zones, when these features are not used. The Create Group VPN option on the Add Zone dialog controls the display on the MANAGE I Connectivity | VPN > Base Settings page. If the option is selected, the VPN-related configurations are displayed; when it is deselected, the configurations are hidden and only the Unique Firewall Identifier displays in the VPN Global Settings section.

Access Point Features

Topics:
- SonicWall Secure Wireless Cloud Management
- WLAN Mesh for Multi-hop Communications (IEEE 802.11s)
- Bluetooth Low Energy Support on SonicWave Appliances
- Secure Cloud Management of SonicWave Appliances

SonicWall Secure Wireless Cloud Management
The SonicWall secure wireless cloud management system is a cloud-based (Software-as-a-Service), disaster-proof wireless network management system. Secure Cloud Management is hosted in a public cloud (for example, AWS) and can be deployed across multiple regions, thereby providing high availability for both server and data.
Secure Cloud Management can be deployed in AWS as depicted in the figure **AWS Cloud Framework**. All services are installed inside a VPC (Amazon Virtual Private Cloud) in which the Secure Cloud Management has complete control over the virtual networking environment, including selection of IP address range, creation of subnets, and configuration of route tables and network gateways.

**AWS Cloud Framework**

The **Wireless Cloud Management** interface has several pages:

- **Dashboard** – Provides a global view, top-N view, and location view for key metrics for SonicWave wireless clients and deployment.
  - **Global AP Status View** – Shows the total number of SonicWaves/ Clients, total traffic, and SonicWave online/offline status.
  - **Top-N View** – Displays:
    - TOP SonicWaves by TX/RX traffic.
    - TOP Wireless clients by TX/RX traffic.
    - TOP SSIDs by TX/RX traffic.
    - TOP Locations by TX/RX traffic.
    - TOP Zones by TX/RX traffic.
    - TOP Operating Systems by TX/RX traffic.
  - **Location View** – Displays a global map and all wireless deployment sites all over the world. Deployment details regarding the total number of SonicWaves and total traffic is displayed via mouseover.
- **Devices** – Has three sub-pages:
  - **Devices** – Displays all registered SonicWaves under the MSSP account on MySonicWall.
  - **Stations** – Monitors the wireless client stations connected to SonicWaves under the tenant. A global filter allows selection of locations/zones, connections status, and operating system types.
  - **Floor Maps** – Displays floor maps for locations under the tenant.
- **Zones & Policies** – Has several sub-pages:
• **Locations** – Creates and manages the tenant/location/zone hierarchy.

• **Zones** – Sets the zone configuration and moves a SonicWave from inventory to zone for cloud management. If the SonicWave is not moved on this page, it remains in the inventory table.

• **Configuration** – Manages the configuration policies attached to zones for SonicWave provisioning. By default, the tenant has the Default Policy.

• **SSID Groups** – Manages SSID groups. An SSID group represents the Virtual Access Point group, which is the container for including many SSIDs, each of which can have different authentication, encryption, and other access control settings.

• **Reports** – has several sub-pages:
  - **Generate** – Generates a report and makes it available for downloading from the cloud.
  - **Options** – Customizes the report according to selected options.

• **Settings** – Controls the login session timeout.

### WLAN Mesh for Multi-hop Communications (IEEE 802.11s)

#### Terminology

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMPE</td>
<td>Authenticated Mesh Peering Exchange</td>
</tr>
<tr>
<td>AP</td>
<td>Access point.</td>
</tr>
<tr>
<td>MESH</td>
<td>A local network topology in which the access point nodes connect directly, dynamically, and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data from/to clients.</td>
</tr>
<tr>
<td>MAP</td>
<td>Mesh Access Point, an access point collocated with a Mesh point.</td>
</tr>
<tr>
<td>MP</td>
<td>Mesh Point, a node supporting wireless mesh service.</td>
</tr>
<tr>
<td>MPP</td>
<td>Mesh Point Portal, the gateway between the wireless mesh network and the enterprise-wired LAN.</td>
</tr>
<tr>
<td>SAE</td>
<td>Simultaneous Authentication of Equals.</td>
</tr>
</tbody>
</table>

#### Topics:

- About WLAN Mesh
- Setting Up a Mesh Network
- Enabling a Multi-Hop Mesh Network
- Active/Active Clustering Full-Mesh

### About WLAN Mesh

IEEE 802.11 standards mainly focus on one-hop infrastructure-based communications, where the stations are directly connected to the access point. In the IEEE 802.11s network, the WLAN mesh is defined as a set of mesh points interconnected via wireless links with the capabilities of automatic topology learning and dynamic path selection. **IEEE 802.11s WLAN Mesh** shows an example of an IEEE 802.11s WLAN mesh. In the figure, there are three classes of wireless nodes, MP, MPP and MAP. The stations do not participate in the WLAN mesh, but they can associate with the mesh APs to connect to the mesh networks. Multiple WLAN meshes can also be connected by the MPP.
IEEE 802.11s WLAN Mesh

There are no defined roles in a mesh — no clients and servers, no initiators and responders. Security protocols used in a mesh must, therefore, be true peer-to-peer protocols where either side can initiate to the other or both sides can initiate simultaneously.

Between peers, 802.11s defines a secure password-based authentication and key establishment protocol called Simultaneous Authentication of Equals. When peers discover each other (and security is enabled), they take part in an SAE exchange. If SAE completes successfully, each peer knows the other party possesses the mesh password and, as a by-product of the SAE exchange, the two peers establish a cryptographically strong key. This key is used with the Authenticated Mesh Peering Exchange to establish a secure peering and derive a session key to protect mesh traffic, including routing traffic.

Setting Up a Mesh Network

NOTE: You can use the SonicWall Secure Cloud Wireless tools to set up a mesh network if your SonicWaves are not managed by a SonicWall firewall.

To set up a mesh network in SonicOS:

1. Enable mesh in the SonicWave profile for your firewall as described in Enabling a Multi-Hop Mesh Network.
2. Connect each SonicWave to this firewall by an Ethernet cable.
3. When a SonicWave’s state becomes operational, disconnect the cable from that appliance.
4. Keep one SonicWave connected to the firewall.
5. Move the disconnected SonicWave to its designated location.
6. Power up all the SonicWaves.
Enabling a Multi-Hop Mesh Network

To enable multi-hop mesh networks:

1. Navigate to MANAGE | Connectivity > Access Points > Base Settings.
2. Scroll to the SonicPoint / SonicWave Provisioning Profiles section.
3. Click on the Edit icon for SonicWave. The Edit SonicWave Profile dialog displays.
4. Click Mesh Networks.
5. Choose the radio to be used for the mesh network from Mesh Radio:
   - 5GHZ Radio
   - 2.4GHZ Radio
6. To enable the radio band Mesh, select Enable Mesh.
7. Enter the SSID for the WLAN network in Mesh SSID.
8. Enter the preshared key in Mesh PSK.
9. Click OK.

Active/Active Clustering Full-Mesh

An Active/Active Clustering Full-Mesh configuration is an enhancement to the Active/Active Clustering configuration option and prevents any single point of failure in the network. All firewall and other network devices are partnered for complete redundancy. Full-Mesh ensures that there is no single point of failure in your deployment, whether it is a device (security appliance/switch/router) or a link. Every device is wired twice to
the connected devices. Active/Active Clustering with Full-Mesh provides the highest level of availability possible with high performance; see Benefits of Active/Active Clustering Full Mesh.

**IMPORTANT:** The routers in the security appliance’s upstream network should be pre-configured for Virtual Router Redundancy Protocol (VRRP). Full Mesh deployments require that Port Redundancy is enabled and implemented.

**Benefits of Active/Active Clustering Full Mesh**

| No Single Point of Failure in the Core Network | In an Active/Active Clustering Full-Mesh deployment, there is no single point of failure in the entire core network, not just for the security appliances. An alternative path for a traffic flow is always available in case there are simultaneous failures of switch, router, security appliance on a path, thus providing the highest levels of availability. |
| Port Redundancy | Active/Active Clustering Full-Mesh utilizes port redundancy in addition to HA redundancy within each Cluster Node, and node level redundancy within the cluster. With port redundancy, a backup link takes over in a transparent manner if the primary port fails. This prevents the need for device level failover. |

**Bluetooth Low Energy Support on SonicWave Appliances**

SonicWave 200 series and 432 series access points support Bluetooth Low Energy (BLE), a wireless personal area network technology that provides considerably reduced power consumption and cost while maintaining a similar communication range to standard Bluetooth appliances.

SonicOS 6.5.4 supports iBeacon and Bluetooth scanning features using the Bluetooth Low Energy radio on SonicWave wireless access points.

**Secure Cloud Management of SonicWave Appliances**

SonicWall Secure WiFi Cloud Management system provides centralized visibility and control over SonicWave wireless access points, without the complexity of wireless controllers or overlay management systems.

Secure WiFi Cloud Management includes the following tools to help you deploy, configure, and seamlessly manage your wireless network:

- WiFi Cloud Manager – Cloud-based management system used to configure, manage, and monitor your wireless network.
- WiFi Planner – Wireless network planning tool used to determine optimal access point placement and optimizes wireless distribution systems and mesh networks.
- SonicWiFi – Mobile app used to register access points, create mesh networks, and troubleshoot access point issues.

The WiFi Cloud Management tools are fully integrated with your Capture Security Center account. Your MySonicWall tenant information and registered devices are imported to each tool simplifying network management.

These features are supported in the SonicOS 6.5.4.3 release:

- Unified visibility and control of the entire network via a single dashboard: wireless, tenant, and security
- Streamlined large networks with tens of thousands of SonicWaves
- Zero-touch provisioning for rapid deployment
- Built-in multi-factored health/diagnostics key index
- Automated network monitoring and reporting
- Intuitive interface eliminates costly training
- Network hierarchy/policy engine – search, inherit, and sync policy/configuration by network hierarchy
- Seamless integration in CSC with administration, tenant, and inventory
- Continuous feature updates delivered from the cloud
- Highly available and secure (Two-Factor Authentication, all packets encryption)

For more information about Secure WiFi Cloud Management of SonicWave appliances, point your browser to the SonicWall Technical Documentation portal at https://www.sonicwall.com/support/technical-documentation and select Secure Cloud Wireless in the Select A Product field.

**CSC Flow Reporting and Visualization Support on SOHO W**

All flow reporting and visualization pages available in TZ300 series and above security appliances are now available in all SOHO series security appliances.

**Expired Certificates Blocked in DPI-SSL Client**

An option has been added to the MANAGE | Security Configuration > Decryption Services > DPI-SSL/TLS Client page:

![DPI-SSL Status](image)

**General Settings**

- Enable SSL Client Inspection
- Intrusion Prevention
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Application Firewall
- Content Filter
- **Always authenticate server for decrypted connections**
- **Allow Expired CA**
- Deployments wherein the Firewall sees a single server IP for different server domains, ex: Proxy setup
- Allow SSL without decryption (bypass) when connection limit exceeded
- Audit new default exclusion domain names prior to being added for exclusion
- Always authenticate server before applying exclusion policy

This option is not selected by default. If it is not selected, DPI-SSL does not use expired or intermediate CAs to verify a server’s certificate. If it is selected, DPI-SSL uses all certificates for verification.

**IMPORTANT:** Before enabling this option, you must first enable **Always authenticate server for decrypted connections**.
Block Login Attempts by IP Address Range

You can now block login attempts based on the number of login attempts by IP address range and not just by user name. New options have been added to the MANAGE | System Setup > Appliance > Base Settings page.

![Login Attempts Configuration](image)

There is an option for just logging the event without the login being blocked.

**NOTE:** This feature applies to local user and built-in administrators only. For LDAP users, the feature is supported only if they are imported to the firewall as local users.

HA synchronization is considered.

This feature applies to CLI logins as well.

Enhanced Logging

Topics:

- Configuration Auditing
- Logging for NAT TCP Connections
- DPI Logged on Packet Level
- Filename Logging
- Log Automation of FTP Settings

Configuration Auditing

In SonicOS 6.5.4, the Enable Enhanced Audit Logging checkbox is available on the MANAGE | System Setup | Appliance > Base Settings page.

When enabled, if the admin makes a configuration change, a log event will occur starting with “Configuration changed:” You can see the log event on the INVESTIGATE | Event Logs page.

Logging for NAT TCP Connections

NAT events using TCP connections are now logged on the INVESTIGATE | Logs > Connection Logs page along with UDP and ICMP connections.

DPI Logged on Packet Level

Syslog event messages now provide a “dpi=0” or “dpi=1” tag which shows whether or not the packet was inspected by DPI-SSL.

The dpi tag indicates that a flow underwent inspection by Deep Packet Inspection.

The dpi tag only applies to Connection Closed Syslog events with the message ID defined as either:

- m=537 if the flow has no URL information, or if CFS was not enabled
Possible values for dpi are:

- 1 = DPI inspection occurred
- 0 = no DPI inspection

**Filename Logging**

This feature allows notification of each filename or URI of interest that has been explicitly identified as App Control processes packets or flows. A new option, **Enable Filename Logging**, has been added to the App Control Global Settings section of the MANAGE | Policies | Rules > App Control page. A new option, **Filename Logging**, also has been added to Firewall > Application Control category on the MANAGE | Logs & Reporting | Log Settings > Base Setup page.

**Log Automation of FTP Settings**

This feature enables logs to be sent to an FTP server. A new section, **FTP Log Automation**, has been added to the MANAGE | Logs & Reporting | Log Settings > Automation page.

**Increased IP Helper Policy Count**

The maximum number of IP helper policies has increased from 128 to 256.

**Enhanced Cipher Control for SSL Communication**

A new SonicOS management interface page, MANAGE | Security Configuration | Firewall Settings > Cipher Control, has been added for controlling both TLS ciphers and SSH ciphers. TLS ciphers can be blocked or allowed, and SSH ciphers can be enabled or disabled.

**Resolved Issues**

This section provides a list of resolved issues in this release.

**CFS**

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>The connection to the IPv6 HTTP server is reset after enabling CFS.</td>
<td>213700</td>
</tr>
</tbody>
</table>

**CLI**

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>The configuration should not be saved when editing an existing DDNS profile with no domain.</td>
<td>214760</td>
</tr>
<tr>
<td>Cannot enable Client DPI-SSL if SSL control is already enabled.</td>
<td>214463</td>
</tr>
</tbody>
</table>
### DPI-SSL

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot add Common Name to the exclusion list in Client DPI-SSL if SSL Control is enabled.</td>
<td>215694</td>
</tr>
<tr>
<td>LAN PC access to some Google (YouTube and Google Translate) websites cannot show the pages in Client DPI-SSL.</td>
<td>213704</td>
</tr>
</tbody>
</table>

### Flow Reports

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Reporting data is not sent to the GMSFlow Server if firewall added from factory default.</td>
<td>215546</td>
</tr>
</tbody>
</table>

### Log

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSA 4600: Missing FW action field in the syslog.</td>
<td>215659</td>
</tr>
<tr>
<td>NSA 5650: CPU utilization goes high due to tWebMain tasks while exporting logs in CSV or TXT format and it takes longer time to download the logs.</td>
<td>212054</td>
</tr>
<tr>
<td>VPN policy tag is missing for VPN user logged-in via L2TP tunnel (remote IP comes from L2TP Server IP Pool).</td>
<td>207416</td>
</tr>
</tbody>
</table>

### Networking

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TZ-300: PPPoE client does not re-connect automatically.</td>
<td>217336</td>
</tr>
<tr>
<td>NSA 3600 running 6.5.2.2 is not able to stop DNS queries for default FQDNs.</td>
<td>216600</td>
</tr>
<tr>
<td>NSA 2600: Unnumbered tunnel interfaces are not listed under SD-WAN member selection until tunnel interface is created.</td>
<td>215560</td>
</tr>
<tr>
<td>Zero Touch process does not work when the HTTP management port is changed on the firewall.</td>
<td>215549</td>
</tr>
<tr>
<td>SD-WAN VPN probes do not work when remote gateway is in DHCP mode.</td>
<td>214781</td>
</tr>
<tr>
<td>The load balancing interface displays as Up on MANAGE</td>
<td>System Setup</td>
</tr>
<tr>
<td>TZ300: Reflexive NAT Policy has same inbound and outbound interface as primary NAT policy, but it should be opposite.</td>
<td>204440</td>
</tr>
</tbody>
</table>

### Switching

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-series SFP+ ports cannot be configured at 1G from the firewall.</td>
<td>216996</td>
</tr>
</tbody>
</table>

### Users

<table>
<thead>
<tr>
<th>Resolved issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSA 2600: Preempt option not coming for multiple users with customized preempt page.</td>
<td>216034</td>
</tr>
<tr>
<td>Gen6: SSL VPN with two-factor one-time password (TOTP) users disconnects after few minutes.</td>
<td>215483</td>
</tr>
<tr>
<td>Gen6: Seeing same users for multiple sessions even though Enforce login uniqueness is enabled.</td>
<td>214263</td>
</tr>
<tr>
<td>File not found! page is always displayed when TOTP user logs into SSL VPN portal page.</td>
<td>213439</td>
</tr>
<tr>
<td>When SSO agent reads from Novell eDirectory, the servers are shown as domain controllers on the firewall.</td>
<td>209441</td>
</tr>
</tbody>
</table>
## Known Issues

This section provides a list of known issues in this release.

### API

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>When monitoring packets in <strong>INVESTIGATE &gt; Tools &gt; Packet Monitor</strong>, intermediate packets cannot be disabled when Monitor intermediate multicast traffic is disabled on the Packet Monitor Configuration dialog.</td>
<td>215158</td>
</tr>
<tr>
<td>There is no egress interface to add for a DHCPv6 policy, and the CLI also does not include this item when showing policies.</td>
<td>214674</td>
</tr>
<tr>
<td>API can not create a DHCPv6 policy (destination no key).</td>
<td>214669</td>
</tr>
<tr>
<td>The raw data response to IP Helper’s protocols and policies statistics are wrong.</td>
<td>214545</td>
</tr>
</tbody>
</table>

### CLI

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI and API cannot show an auto-generated NetBIOS policy.</td>
<td>215247</td>
</tr>
</tbody>
</table>

### DPI-SSL

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downloading a large file may be slow or time out when DPI-SSL is enabled.</td>
<td>218627</td>
</tr>
<tr>
<td>Firewall may cease operation if admin switches from a DPI-SSL exclusion policy straight to inclusion.</td>
<td>218544</td>
</tr>
<tr>
<td>DPI-SSL Client does not work when HTTPS server used in combination with XS09V1 self-signed certificate.</td>
<td>218383</td>
</tr>
<tr>
<td>In rare cases, high latency might be observed when accessing HTTPS sites with Client DPI-SSL CFS Enforcement.</td>
<td>217716</td>
</tr>
<tr>
<td>The websites’ certificates are not replaced by DPI-SSL certificate when using 3G/4G card as WWAN interface.</td>
<td>216253</td>
</tr>
</tbody>
</table>

### Geo-IP/Botnet

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Botnet list is not present after the upgrade from 6.5.3.1-48n to 6.5.4.3-34n.</td>
<td>218784</td>
</tr>
</tbody>
</table>
## High Availability

**Known issue**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>218686</td>
<td>User might be asked to re-authenticate when a user session is active and the secondary firewall takes-over and becomes-active.</td>
</tr>
<tr>
<td>218396</td>
<td>User account name is not shown on standby unit of HA pair in WAN GroupVPN.</td>
</tr>
<tr>
<td>216339</td>
<td>The <strong>HA Data Link</strong> should not be displayed on the **MONITOR</td>
</tr>
</tbody>
</table>

## Log

**Known issue**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>213068</td>
<td>FTP server cannot obtain FTP Log in site-to-site VPN.</td>
</tr>
</tbody>
</table>

## Networking

**Known issue**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>218779</td>
<td>SonicOS web management interface is not accessible via X1 IP after upgrade from 6.2.7.1-23n to 6.5.4.3-34n and requires an additional firewall restart.</td>
</tr>
<tr>
<td>218357</td>
<td>Connection is not blocked and event is not logged when admin enables Detect SSLv3 and Detect TLSv1 and enables Client DPI SSL.</td>
</tr>
<tr>
<td>217709</td>
<td>Unnumbered tunnel interface should not be allowed to delete if it is already used in SD-WAN groups.</td>
</tr>
<tr>
<td>216606</td>
<td>Firewall web management interface is not accessible with legacy TLS 1.1 on 6.5.4.2-27n in certain browsers.</td>
</tr>
<tr>
<td>215976</td>
<td>Existing connections are disconnecting when enabling Load balancing.</td>
</tr>
<tr>
<td>215851</td>
<td>Interface Load Balanced state is not displayed as disabled after disabling the feature in the web management interface.</td>
</tr>
<tr>
<td>215775</td>
<td>Existing sessions are disconnecting when new route qualifies.</td>
</tr>
<tr>
<td>215088</td>
<td>Network Monitor policy with Ping and TCP Probe type does not work when it matches SD-WAN route policy with two member interfaces configured for SD-WAN group.</td>
</tr>
<tr>
<td>212424</td>
<td>The DHCP Server X0 scope is enabled after restarting the firewall.</td>
</tr>
<tr>
<td>212009</td>
<td>IP helper over VPN does not work when configuring non-X0 as local subnet in DHCP server side.</td>
</tr>
</tbody>
</table>

## SonicPoint

**Known issue**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>218631</td>
<td>The <strong>Access Points &gt; Base Settings</strong> page is not displayed for limited admin users.</td>
</tr>
</tbody>
</table>

## SSL VPN

**Known issue**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>217748</td>
<td>A Telnet bookmark lost connection after clicking S-shield and setting it to full screen.</td>
</tr>
<tr>
<td>216713</td>
<td>Issues observed when accessing bookmarks as the last licensed user.</td>
</tr>
<tr>
<td>216081</td>
<td>Unable to Telnet to networking device (router) through SSL VPN bookmark.</td>
</tr>
</tbody>
</table>
### Switching

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to add N-Series switches if enable password is configured on the switch.</td>
<td>215381</td>
</tr>
<tr>
<td>When LAG with HA is configured, some connection issues are observed.</td>
<td>213752</td>
</tr>
</tbody>
</table>

### Users

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>For a certain zone both “User authentication” and “Guest services” may not work if both are selected together.</td>
<td>217958</td>
</tr>
<tr>
<td>TOTP: Unbind does not take effect for a specific domain user.</td>
<td>216866</td>
</tr>
<tr>
<td>With Client Certificate Check, Chrome/Firefox cannot log in after verifying the certificate successfully, and the message “This browser window does not appear to be the one most recently used to log in” is displayed.</td>
<td>214787</td>
</tr>
<tr>
<td>Local User account lockout will fail if the User authentication method is RADIUS+Local Users or LDAP+Local Users.</td>
<td>213620</td>
</tr>
<tr>
<td>SonicOS failed to re-add a local user to local groups and displayed error messages.</td>
<td>211243</td>
</tr>
</tbody>
</table>

### VPN

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Site-to-Site VPN traffic still passes through the primary WAN after failover to the secondary WAN.</td>
<td>213928</td>
</tr>
<tr>
<td>OSPF redistribute by VPN: Numbered tunnel interface cannot be switched to secondary tunnel interface when primary tunnel interface is down, and the route database is not updated.</td>
<td>213768</td>
</tr>
<tr>
<td>WAN GroupVPN is disabled by default, which causes an issue.</td>
<td>212205</td>
</tr>
</tbody>
</table>

### Web Management Interface

<table>
<thead>
<tr>
<th>Known issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>The hyperlink provided in the System Status page does not point to the correct URL.</td>
<td>216599</td>
</tr>
</tbody>
</table>
System Compatibility

This section provides additional information about hardware and software compatibility with this release.

Wireless 3G/4G Broadband Devices

SonicOS 6.5.4 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see:


GMS Support

A future version of SonicWall GMS will support management of the new features in SonicOS 6.5.4.

WAN Acceleration / WXA Support

The SonicWall WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with SonicWall security appliances running SonicOS 6.5.4. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser Support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher
- IE Edge or IE 10.0 and higher
- Safari 10.0 and higher running on non-Windows machines

**NOTE:** On Windows machines, Safari is not supported for SonicOS management.

**NOTE:** Mobile device browsers are not recommended for SonicWall appliance system administration.

Product Licensing

SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at https://mysonicwall.com.
Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the SonicOS 6.5 Upgrade Guide available on the Support portal at https://www.sonicwall.com/support/technical-documentation.

SonicWall Support

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

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

The Support Portal enables you to:

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

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