

SonicWall® SonicOS 6.5.4.4 Release Notes

July 2019, updated August 2019

These release notes provide information about the SonicWall® SonicOS 6.5.4.4 release.

Topics:

- [About SonicOS 6.5.4.4](#)
- [Security Advisory](#)
- [Supported Platforms](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [System Compatibility](#)
- [Product Licensing](#)
- [Upgrading Information](#)
- [SonicWall Support](#)

About SonicOS 6.5.4.4

SonicWall SonicOS 6.5.4.4 fixes a number of issues and vulnerabilities found in previous releases. For more information, see the [Resolved Issues](#) section.

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>.

Security Advisory

Ensuring the security of our customers is a responsibility we take seriously at SonicWall. Please review the security advisory and update your SonicWall firewall per the advisory.

Security Advisory: https://www.sonicswall.com/support/product-notification/?sol_id=190717234810906

Supported Platforms

SonicOS 6.5.4.4 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

Resolved Issues

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

CFS

Resolved issue	Issue ID
Under a corner case condition, a memory leak can occur when deleting a CFS action object.	219526
A corrupted entry can be created when a new URL or keyword is added to the CFS allowed or forbidden list.	219246, 219715

DPI-SSL

Resolved issue	Issue ID
HTTPS file download speed drops dramatically when Client DPI-SSL is enabled. Downloading a large file may be slow or time out.	219430, 218627
Firewall may cease operation if admin switches from a DPI-SSL exclusion policy straight to inclusion.	218544
DPI-SSL stops working over time due to Memory Low Condition.	217613, 216644, 216047, 214614, 214100

High Availability

Resolved issue	Issue ID
User might be asked to re-authenticate when a user session is active and the secondary firewall takes over and becomes active.	218686
User account name is not shown on standby unit of HA pair in WAN GroupVPN.	218396

Networking

Resolved issue	Issue ID
Disable Source Port Remap in NAT policy configuration cannot be turned off.	219926
A misconfigured DHCP server on an external router causes the firewall to reboot. Occurs when the DHCP server does not have a subnet mask configured for the IP address range provided to the WAN interface of the SonicWall firewall.	219488
Multiple TFTP transactions cannot be carried out on a single TFTP control connection.	218732

PCI Scan False Positive

Resolved issue	Issue ID
PCI scan is failing for port 443 and 8443 because “a known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm”. Occurs when an SSL certificate signed by GoDaddy is imported on the appliance for SSL VPN and administration purposes. “The Go Daddy Group, Inc.” with Serial Number-00 is present in the built-in trusted root certificates which are signed using SHA-1 hashing algorithm and checked in the certificate chain, causing the PCI scan to fail. Legacy browsers are most likely to show this. For more information, see the Knowledge Base article at https://www.sonicwall.com/support/knowledge-base/?sol_id=190624121900833	218308

SSL VPN

Resolved issue	Issue ID
Unable to delete bookmarks from the SSL VPN virtual office portal.	217985

System

Resolved issue	Issue ID
Under corner case conditions, SonicOS might restart when enabling an additional syslog server.	219375, 218596

Users

Resolved issue	Issue ID
LDAP domain and user configuration might be cleared upon upgrade to SonicOS 6.5.4.3.	219014, 220870

VoIP

Resolved issue	Issue ID
Under a corner case condition, the firewall might restart upon encountering an error while processing H.323 traffic.	218384

VPN

Resolved issue	Issue ID
Easy VPN tunnel might fail to be established as the Phase2 security association is not initiated.	219938

Known Issues

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

API

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

CLI

Known issue	Issue ID
CLI and API cannot show an auto-generated NetBIOS policy.	215247

DPI-SSL

Known issue	Issue ID
When visiting certain websites, the browser displays a CA certificate error and the user must agree to the risk in order to continue to the website. Occurs when Client DPI-SSL presents a self-signed CA certificate generated using Go Daddy Class 2 Certification Authority to the client computer for certain websites. However, the Go Daddy Class 2 Certification Authority was removed from the list of Trusted CAs due to a weak signing algorithm.	220615
In certain scenarios, downloading large files might not succeed when Server DPI-SSL is enabled.	220430
DPI-SSL Client does not work when HTTPS server used in combination with X509V1 self-signed certificate.	218383
In rare cases, high latency might be observed when accessing HTTPS sites with Client DPI-SSL CFS Enforcement.	217716
The websites' certificates are not replaced by DPI-SSL certificate when using 3G/4G card as WWAN interface.	216253

Geo-IP/Botnet

Known issue	Issue ID
Dynamic Botnet list might not be present after the upgrade to 6.5.4-based releases.	218784

High Availability

Known issue	Issue ID
The HA Data Link should not be displayed on the MONITOR Current Status > High Availability Status page as there is only a Control Link for the TZ350 Wireless.	216339

Log / Syslog

Known issue	Issue ID
The DELETE ALL function might not work correctly when there is more than one page of servers listed in the Syslog Servers table on the MANAGE Log Settings > SYSLOG page, and the DELETE ALL button is clicked on a page other than the first page.	220409
In certain scenarios, syslog messages might not be sent to GMS over a site-to-site VPN tunnel.	220405
The FTP log is not transferred to the configured FTP Server over a site-to-site VPN tunnel.	213068

Networking

Known issue	Issue ID
The Enable IPv6 option might not work correctly when it is selected multiple times or when ACCEPT is clicked multiple times on the System > Administration page.	219931
An SD-WAN route is not disabled or greyed out when all interfaces in the Path Selection Profile (PSP) have a status of Not Qualified.	219900
The SonicOS web management interface is not accessible via X1 IP after upgrade from 6.2.7.1-23n to 6.5.4-based releases and requires an additional firewall restart.	218779
Connection is not blocked and event is not logged when the admin enables Detect SSLv3 and Detect TLSv1 and enables Client DPI SSL.	218357
Unnumbered tunnel interface should not be allowed to delete if it is already used in SD-WAN groups.	217709
Firewall web management interface is not accessible with legacy TLS 1.1 on 6.5.4.x in certain browsers.	216606
Existing connections are disconnecting when enabling Load balancing.	215976
Existing sessions are disconnecting when new route qualifies.	215775
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.	215088
IP helper over VPN does not work when configuring non-X0 as local subnet in DHCP server side.	212009

SonicPoint/SonicWave

Known issue	Issue ID
The Access Points > Base Settings page is not displayed for limited admin users.	218631

SSL VPN

Known issue	Issue ID
Issues observed when accessing bookmarks as the last licensed user.	216713
Unable to Telnet to networking device (router) through SSL VPN bookmark.	216081

Switching

Known issue	Issue ID
Unable to add N-Series switches if enable password is configured on the switch.	215381
When LAG with HA is configured, some connection issues are observed.	213752

Users

Known issue	Issue ID
On a connect failure, LDAP does not retry with a different IP address when an LDAP server has more than one.	220325
A connectivity test of a RADIUS server failed after adding a LAN zone partition selection policy.	219737
For a certain zone both "User authentication" and "Guest services" may not work if both are selected together.	217958
TOTP: Unbind does not take effect for a specific domain user.	216866
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.	214787
Local User account lockout will fail if the User authentication method is RADIUS+Local Users or LDAP+Local Users .	213620
SonicOS failed to re-add a local user to local groups and displayed error messages.	211243

VPN

Known issue	Issue ID
Remote VPN networks might not be reachable in certain conditions after enabling and configuring GMS.	220398
IPv6 Site-to-Site VPN traffic still passes through the primary WAN after failover to the secondary WAN.	213928
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.	213768
WAN GroupVPN is disabled by default, which causes an issue.	212205

Web Management Interface

Known issue	Issue ID
The hyperlink provided in the System > Status page does not point to the correct URL.	216599

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:

<https://www.sonicwall.com/en-us/support/knowledge-base/170505473051240>

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.4 requires GMS 8.7 SP1 for management of firewalls using 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

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

i | **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>.

Copyright © 2019 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.


The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.


For more information, visit <https://www.sonicwall.com/legal>.

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/eupa>.

Legend

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

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

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

Last updated: 8/9/19

232-004970-00 Rev B