SonicWall® SonicOS 6.5.4.7

Release Notes

September 2020

These release notes provide information about the SonicWall® SonicOS 6.5.4.7 release.

Topics:

About SonicOS 6.5.4.7

SonicWall SonicOS 6.5.4.7 fixes a number of issues, including potential 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.

Supported Platforms

SonicOS 6.5.4.7 is supported on the following SonicWall appliances:

- NS*a* 9650
- NS*a* 9450
- NS*a* 9250
- NS*a* 6650
- NS*a* 5650
- NS*a* 4650
- NS*a* 3650
- NS*a* 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.

Dell X-Series Switch Interoperability

Resolved issue	Issue ID
Wireless clients connected to a Dell X-Series switch are not able to reach the WAN after upgrading the firewall from SonicOS 6.5.4.5 to 6.5.4.6. **Workaround**: Remove and re-add the X-Series switch and re-configure the X-Series switch port.	GEN6-1282

DPI-SSL

Resolved issue	Issue ID
SonicOS may unexpectedly restart due to hitting a corner case condition in DPI-SSL processing. Occurs when Client DPI-SSL is enabled after firmware update to 6.5.4.6-79n.	GEN6-1268

Networking

Resolved issue	Issue ID
A PortShield group stopped working after firmware update to 6.5.4.6-79n.	GEN6-1308

SSL VPN

Resolved issue	Issue ID
Mobile Connect clients running on Android and Chromebook are able to connect to the firewall, but traffic is not forwarded.	GEN6-1285
After upgrading to SonicOS 6.5.4.6, NetExtender sessions are exhibiting slower performance.	GEN6-1417

SonicWall Switch

Resolved issue	Issue ID
Traffic from the access VLAN member port does not make it to the firewall. Occurs when a SWS14-48FPoE Switch is connected to the firewall and Switch ports are configured as access VLAN. DHCP clients on these ports do not receive DHCP addresses.	SWO-1315

Known Issues

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

DPI-SSL

Known issue	Issue ID
The WAN side SMTPS client often cannot successfully send mail to the LAN side SMTP server when cleartext is enabled in the DPI-SSL server. **Workaround**: Disable the cleartext option.	GEN6-853

Gateway Anti-Virus

Known issue	Issue ID
PuTTY uses a new EXE signature that causes GAV to not recognize putty.exe as an executable file.	GEN6-1526

High Availability

Known issue	Issue ID
In a High Availability pair, the standby firewall cannot be managed using its monitoring IP address. Occurs after restarting the standby firewall.	GEN6-281
In a High Availability pair with Stateful Synchronization enabled, a new FTP connection is established after a failover caused by disconnecting X0 on the active unit.	GEN6-1733

User Interface

Known issue	Issue ID
Not all Address Objects are removed when a large number are selected by the administrator to be removed. **Workaround**: Delete Address Objects in batches smaller than 50.	GEN6-38
Firmware backup cannot be created when managing the firewall with the Edge browser. **Workaround**: Manage the firewall with Firefox, Chrome or Internet Explorer.	GEN6-554
Under Cloud Backup, clicking the **Delete all configurations** button for a selected firmware version can cause an error. **Workaround**: Manually delete all the cloud backup configuration files under the selected firmware version to be deleted.	GEN6-1189
The error message, “Error: The Subnet Mask must be wider than 255.255.252.0” is displayed when configuring a WLAN zone interface in PortShield Switch Mode with **PortShield to** set to another WLAN interface in Static IP mode with Subnet Mask 255.255.255.0.	GEN6-1773

Users

Known issue	Issue ID
Authentication fails when Time-based One-Time Password (TOTP) is enabled for a local user, and the error message, “too many login failed attempts” is displayed after entering the authenticator code three times.	GEN6-1756

VPN

Known issue	Issue ID
The Global VPN Client (GVC) cannot connect to the firewall when the WAN Group VPN policy is configured to use the certificate authentication method and the **OCSP checking** option is enabled. **Workaround**: Disable the **OCSP checking** option.	GEN6-768

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/support/knowledge-base/what-wireless-cards-and-broadband-devices-are-supported-on-sonicwall-firewalls-and-access-points/170505473051240/

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.4 requires GMS 8.7 SP1 or GMS 9.2 for management of firewalls using the 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, Edge or Safari browsers for administration of SonicOS. This release supports the following web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher
- Edge 81.0 and higher
- 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.

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 and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support
- 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.

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: 9/29/20

232-005465-00 Rev A