

SonicWall® SonicOS 6.5.1.3 Release Notes September 2018

These release notes provide information about the SonicWall® SonicOS 6.5.1.3 release.

Topics:

- [About SonicOS 6.5.1.3](#)
- [Supported Platforms](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [System Compatibility](#)
- [Product Licensing](#)
- [Upgrading Information](#)
- [SonicWall Support](#)

About SonicOS 6.5.1.3

SonicOS 6.5.1.3 is a maintenance release that fixes a number of issues found in previous releases. For more information, see the [Resolved Issues](#) section.

This release provides the same features and contains all the resolved issues that were included in previous releases of SonicOS 6.5.1. For more information, see the previous release notes, available on [MySonicWall](#).

Supported Platforms

SonicOS 6.5.1.3 is supported on these SonicWall appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- NSa 5650
- NSa 4650
- NSa 3650
- NSa 2650
- TZ600
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ300 / TZ300 Wireless
- SOHO Wireless

Resolved Issues

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

High Availability

Resolved issue	Issue ID
Traffic may be dropped on an HA failover to standby if it fails to allocate unique remap ports for the NATed traffic. Occurs when the HA standby unit does not correctly release allocated NAT remap ports during the connection state synchronization. Over a period of time, the available NAT remap ports become exhausted. Once exhausted, no ports are available to be allocated for the new connections, causing it to be dropped.	207729

Management Interface

Resolved issue	Issue ID
The management interface displays a <code>This browser window does not appear to be the one most recently used to log in</code> warning. Occurs when logging in to the firewall over HTTPS with a new browser window.	201569
The management interface stops responding intermittently while browsing/editing on the management interface. Occurs when a large IP Report needs to be generated and loaded onto the MONITOR Dashboard page.	200038

Networking

Resolved issue	Issue ID
The SFP+ interface does bring the link up as 10Gbps. Occurs with certain TwinAx modules and network switches.	206485
The firewall may periodically restart without reporting diagnostic information. Occurs when certain physical interfaces have been administratively shutdown.	206309
TCP traffic sent by SonicOS over SSL VPN may fail to be received by NetExtender. Occurs when a smaller MSS is requested for the TCP connection by NetExtender than that of the outgoing network interface.	205364
SSL-VPN fails PCI scan for CVE-2009-3555. Occurs during TLS session renegotiation. For further information, see CVE-2009-3555 .	202309

SSL VPN

Resolved issue	Issue ID
Bookmarks are not displayed. Occurs when logging into the console and the bookmarks were created with the Command Line Interface (CLI) either from local users or local groups.	205956

System

Resolved issue	Issue ID
While processing NetBios traffic with Security services enabled (GAV), the firewall may restart often without a specific task failure or stack trace information. Occurs when either GAV processes malformed NetBIOS traffic/packets or NetBIOS traffic includes a transfer of files with certain characteristics.	206711
The firewall restarts when DPI-SSL is enabled on certain NSA and SuperMassive models. Occurs when DPI-SSL makes certain accesses in internal extended memory.	204880
The firewall restarts during signature download. Occurs due to accessing incorrect state information after a failed connection.	203737
SonicWall TZ series appliances exhibit high core 0 utilization, causing the unit to become unresponsive for management and websites to load slowly. Occurs when the appliance is performing multiple web server-related tasks.	199726

Users

Resolved issue	Issue ID
SonicWall fails to identify hosts' user groups with SSO. Occurs when the SonicWall LDAP schema is set to use Novell and SonicWall sends requests to Novell using Microsoft active directory schema.	208680
User group memberships are not properly set when looked up via LDAP immediately after upgrade to 6.5.n, and this continues until the device is restarted. Occurs after upgrading to SonicOS 6.5.n and when using LDAP for user group lookup with domain user groups having been imported (or manually configured) before the upgrade and having not restarted the appliance since the upgrade.	206528

Vulnerability

Resolved issue	Issue ID
Service Objects, Address Objects and NAT/Access Rules have a vulnerability; for further information, see CVE-2018-5280 .	206810

Known Issues

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

CFS

Resolved issue	Issue ID
With Content Filtering Service enabled, under certain corner-case conditions, the CFS Server Status is reported as not responding in the management interface, and the firewall does not generate the request traffic (UDP port 2257) to the CFS server. The Diagnostic/Check Network Settings to test Content filtering is also impacted. Occurs intermittently after extended periods of usage.	205289

DPI-SSH

Known issue	Issue ID
Blocking of attachments and append message actions may not work with SMTP over SSL. Occurs when SSL Client Inspection is enabled and the Application Firewall option is selected on the DPI-SSL/TLS Client page with an accompanying App Rule policy configured to block attachments and add text.	198590
Skip CFS Category-based Exclusion may not work correctly. Occurs when a common name is added on the DPI-SSL/TLS Client page with the Skip CFS Category-based Exclusion option selected. Category 20. (Online Banking) is excluded, and then a LAN-side PC attempts to access the excluded common name.	198185
CFS Category-based Inclusions/Exclusions may not exclude correctly. Occurs when SSL Client Inspection is selected on the DPI-SSL/TLS Client page, Category 29. (Search Engines and Portals) is excluded on the CFS Category-based Exclusions/Inclusions dialog, and then a LAN-side PC accesses a search engine. DPI-SSL still occurs.	196892

High Availability

Known issue	Issue ID
The default route doesn't sync to the idle firewall after the primary WAN is unavailable. Occurs when the default route gets modified by interface state changes.	209291
Virtual MAC addresses cannot be updated on the idle firewall. Occurs when manually changing the virtual MAC address and the Enable Virtual MAC option is already enabled.	206623

Logging

Known issue	Issue ID
Not able configure Maximum Events Per Second and Maximum Bytes Per Second . Occurs when a SYSLOG server has not been configured.	208498
On the INVESTIGATE Logs > Appflow Logs page, selecting Chart View from the Display Options icon displays a blank page with the error, Requests to the server have been blocked by an extension. Occurs when using a Chrome browser.	208389

Management Interface

Known issue	Issue ID
JS error when viewing the MONITOR Current Status > System Status page Occurs when viewing the page on a SOHO W firewall.	206529

SSL VPN

Known issue	Issue ID
When editing a bookmark and then saving it without changing the bookmark name, this prompt displays: <code>The bookmark name is duplicate with existing ones.</code> Workaround: deleting the bookmark and then adding it again is an option in addition to a simple name change with the new edits.	209854
Virtual Assist fails to download from the user portal. Occurs when attempting to download Virtual Assist by clicking the Virtual Assist icon. The message, <code>An add-on for this website failed to run,</code> displays.	193798

Users

Known issue	Issue ID
Users cannot log in as a domain user if a local non-domain user object exists that uses special characters. Occurs when a domain user name contains <code>@</code> , <code>/</code> , or <code>\</code> characters.	209842
The default partition policy changes, causing the partition feature to not work. Occurs when adding a remote-user partition policy from the CLI.	197455

VOIP

Resolved issue	Issue ID
SIP calls to the same destination may fail. Occurs with SIP TCP transformation checked when making a second series of calls to the same destination within a short period of time.	202700

VPN

Resolved issue	Issue ID
A VPN tunnel interface does not come up when the X5 interface is used. Occurs on TZ 500 and TZ 600 appliances.	209361

Wireless

Known issue	Issue ID
Wireless PC clients cannot connect to WiFi. Occurs when the firewall is configured with WPS EAP and with two RADIUS servers in different LAN networks.	206808

X-series switch

Known issue	Issue ID
Adding a dedicated link with a VLAN sub-interface does not add the internal VLAN for the dedicated link in the child switch. Occurs when adding the dedicated link in a dedicated uplink topology for Daisy-chained Dell X-switches.	205909
Port Shield configuration for X1052 has errors. Occurs when a Dell X1052 switch is connected to a Gen6/Gen6.5 firewall with X-Series Configuration enabled. The X1052 switch has 10G, 1G FDX, and 1G copper-only slots, but the NSA 3600 treats all ports on the X1052 as 10G.	200619

System Compatibility

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

Wireless 3G/4G Broadband Devices

SonicOS 6.5.1 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 6.5.1.3 requires GMS 8.5 or later for management of firewalls using the features in SonicOS 6.5.1.1.


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 6.5.1.3. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser Support

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 platforms 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 © 2018 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: 9/19/18

232-004512-00 Rev A