SonicWall® SonicOS 6.5.1.5

Release Notes

July 2019

These release notes provide information about the SonicWall® SonicOS 6.5.1.5 release.

Topics:

- About SonicOS 6.5.1.5
- Security Advisory
- Supported Platforms
- Resolved Issues
- Known Issues
- System Compatibility
- Product Licensing
- Upgrading Information
- SonicWall Support

About SonicOS 6.5.1.5

SonicOS 6.5.1.5 is a General Release that provides protection against certain vulnerabilities and supports cloud management for the SonicWave 432 series. For more information, see the Security Advisory and Resolved Issues sections.

This release provides the same features and contains all the resolved issues that were included in previous releases of SonicOS (that is, SonicOS 6.5.1.*x*, SonicOS 6.5.0.*x*, SonicOS 6.2.9.*x*, and SonicOS 6.2.7.*x*).

For a list of resolved issues in previous SonicOS releases, see the previous release notes, available on MySonicWall at: https://www.mysonicwall.com/.

For a complete list of new features in SonicOS 6.5.1, please refer to the *SonicWall® SonicOS 6.5.1.1 Release Notes*.

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.sonicwall.com/support/product-notification/?sol_id=190717234810906

Supported Platforms

SonicOS 6.5.1.5 is supported on these SonicWall appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- NS*a* 5650
- NS*a* 4650
- NS*a* 3650
- NS*a* 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.

Certificates

Resolved issue	Issue ID
Administrators without full permissions can download imported certificates. Occurs when administrators who are not in the SonicWall Administrators user group attempt to download imported certificates.	211749

Encryption

Resolved issue	Issue ID
The TLS Padding (Zombie POODLE and GOLDENDOODLE) and ROBOT attack vulnerabilities exist in SonicOS. Occurs when a connection to the appliance uses cipher block-chaining (CBC).	215940

Networking

Resolved issue	Issue ID
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

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.	218308

SonicWave

Resolved issue	Issue ID
With the launch of SonicWall Wireless Cloud Management, SonicOS 6.5.1 needs to support SonicWave 432 series cloud compatibility as well as SonicWave management through the firewall.	217724

Known Issues

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

CFS

Known issue	Issue ID
With Content Filtering Service (CFS) 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 affected. Occurs only in L2TP-enabled deployments.	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 **MANAGE | System Setup > 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 > Common Name** 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 **Enable 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

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

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 to 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
A JavaScript error occurs 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: `The bookmark name is duplicate with existing ones`. **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. The message, `An add-on for this website failed to run`, displays. Occurs when attempting to download Virtual Assist by clicking the **Virtual Assist** icon.	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 @, /, or \ 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

Known 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

Known 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 6.5.1.5 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 6.5.1.5 requires GMS 8.5 or later for management of firewalls using the features in SonicOS 6.5.1.x.

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 6.5.1.5. 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.

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: 7/25/19

232-004898-00 Rev A