SonicWall® SonicOS 6.5.1.15

Release Notes

April 2022

These release notes provide information about the SonicWall® SonicOS 6.5.1.15 release.

Topics:

About SonicOS 6.5.1.15

SonicWall SonicOS 6.5.1.15 provides a number of fixes for potential vulnerabilities found in previous SonicOS releases on SonicWall enterprise-class network security appliances. See the Resolved Issues section for information.

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

Supported Platforms

SonicOS 6.5.1.15 is supported on the following SonicWall appliances:

- NS*sp* 12800
- NS*sp* 12400
- SuperMassive 9800

ⓘ **NOTE:** See Upgrading Information on page 5 for the minimum ChassisOS and ChassisROM versions required for upgrading to SonicOS 6.5.1.15.

Connections Scalability in 6.5.1.15

Connections scalability between SonicOS 6.4.0.0 and SonicOS 6.5.1.15 is shown below:

Connections Scalability

Model	Max SPI Connections (2.5x Scalability)		Max DPI Connections (2.5x Scalability)		Max DPI-SSL Connections (13x Scalability)	
	SonicOS 6.4.0.0	***SonicOS 6.5.1.15***	***SonicOS 6.4.0.0***	***SonicOS 6.5.1.15***	***SonicOS 6.4.0.0***	***SonicOS 6.5.1.15***
SM 9800	8 M	20 M	3 M	8 M	48 K	650 K
NS*sp* 12400	16 M	40 M	6 M	16 M	100 K	1.3 M
NS*sp* 12800	32 M	80 M	12 M	32 M	200 K	2.6 M

Resolved Issues

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

Resolved issue	Issue ID
The OpenSSL library can enter an infinite loop when parsing an invalid certificate and can result in a Denial-of-Service (DoS) to the application.	GEN6-3363
Sensitive information about wireless access points may be exposed via SNMP.	GEN6-3322
Cloud backups are not shown on the **Device > Settings > Firmware and Settings** page and new Cloud backups cannot be created.	GEN6-3208

Known Issues

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

Downgrade

Known issue	Issue ID
Firmware downgrade from 6.5.1.8 to 6.4.0.0-24n is not supported. **Workaround**: Load firmware image in Safe Mode and boot with factory defaults.	213198

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. **Workaround**: User must agree to the certificate warning in order to continue to the website.	220615
A website's certificate is not replaced by a DPI-SSL certificate when accessing Google and Mozilla websites. Related policies such as CFS will not work in this case. Occurs when Client DPI-SSL is enabled on the LAN zone and then the websites are accessed. **Workaround**: Block UDP port 443.	212184

GRE

Known issue	Issue ID
An ICMP packet that is de-encapsulated from a GRE packet received on blade 2 is dropped after being forwarded and processed on blade 1.	209515

High Availability

Known issue	Issue ID
After failover in HA, the secondary appliance is unable to connect to the AppFlow Server.	209509

IPv6

Known issue	Issue ID
Type of Service (TOS)/Mask does not work in an IPv6 route policy.	189137
An IPv6 BGP peer fails to establish an IPv4 BGP peer as a BGP neighbor when the IPv4 BGP peer is using MD5 authentication.	205025

Networking

Known issue	Issue ID
SonicWall DHCP server responds incorrectly to a DHCP discover packet received with the unicast bootp flag set. The DHCP offer is sent to 255.255.255.255 even when the discover packet has the unicast flag set. **Workaround**: Contact SonicWall Technical Support for assistance with enabling the “Use unicast dst ip address and link-layer address when unicast flag is set” internal setting.	219918

OSPF

Known issue	Issue ID
Failed to establish an OSPF neighbor when OSPF is enabled on a VLAN interface or trunk VLAN interface.	207138

Security Services

Known issue	Issue ID
In certain UFTP file transfers, one packet is never delivered no matter how many times it is retransmitted unless it is re-encrypted.	222758

SSO-API

Known issue	Issue ID
The API client list does not show in the partition configuration page. **Workaround**: Edit the partition in a third-party API configuration window.	208041

User Interface

Known issue	Issue ID
Cannot assign group membership and VPN access to new user due to web management interface issue. Occurs when accessing the web management interface in Chrome and adding a user or group from the **MANAGE | Users > Local Users & Groups** page, on the **Groups** or **VPN Access** screen of the **Add User** dialog or on the **VPN Access** screen of the **Add Group** dialog. **Workaround**: Use Firefox or Internet Explorer for web management.	222540

Users

Known issue	Issue ID
RDP bookmark login fails when the user enters the correct credentials. **Workaround**: Edit the IPv6 RDP bookmark and enable **Automatically log in**, then configure the correct credentials as Custom Credentials.	208983
User login is denied due to the user not having privileges for login when the same user is added to a local group and **Use LDAP to retrieve user group info** is selected.	208045
When an Authentication Partition is enabled, App Control cannot block the specified domain user. **Workaround**: Either do not enable Authentication Partition, or specify a domain group in the **Included Users/Groups** field.	204202

System Compatibility

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

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.1.15 requires GMS 8.6 or higher for management of firewalls using the features in SonicOS 6.5.1.15.

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.

Supported Client Versions

- NetExtender Windows Client: 8.6.265
- NetExtender Linux Client: 8.6.801
- SSO agent: 4.1.6
- TSA agent: 4.0.16
- GVC: 4.10.2.0428
- Capture client: 1.0.24

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

On SuperMassive 9800, the minimum ChassisOS and ChassisROM (FailSafe) versions required or recommended for upgrading to SonicOS 6.5.1.15 are:

- ChassisOS 6.0.4.2 (required)
- ChassisROM (FailSafe) 6.2.2.1 (recommended)

On NS*sp* 12000 series, the minimum ChassisOS, ChassisROM (FailSafe), and BMC versions required for upgrading to SonicOS 6.5.1.15 are:

- ChassisOS 6.0.7.7
- ChassisROM (FailSafe) 6.2.4.3
- BMC 3.3

ⓘ **NOTE:** The ChassisOS Apps version 6.1.1.10 is embedded in SonicOS 6.5.1.15 on NS*sp* 12000 series, and ***is not backward compatible*** to the previous versions of ChassisROM (FailSafe) and ChassisOS.

ⓘ **NOTE:** The BMC version is not displayed in SonicOS. BMC stands for Baseboard Management Controller and is used to gather the following sensor values and control the hardware.

- Temperature
- Fan
- Power up and down chassis
- Power up and down blades

These sensor values are displayed in SonicOS.

The ChassisOS, ChassisROM (FailSafe), and ChassisOS Apps versions are displayed in the SonicOS SafeMode page. For further information, contact SonicWall Technical Support.

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, accessing SafeMode, and importing configuration settings from another appliance, see the *SonicOS 6.5 NSsp12k-SM9800 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/end-user-product-agreements.

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: 4/20/22

232-005835-00 Rev A