SonicWall® SonicOS 6.5.0.2-37-158 for NS$_v$ Series

Release Notes

June 2018

These release notes provide information about the SonicWall® SonicOS 6.5.0.2-37-158 for NS*v* Series release.

Topics:

- About SonicOS 6.5.0.2-37-158 for NS$_v$ Series
- Supported Platforms
- Resolved Issues
- Known Issues
- System Compatibility
- Product Licensing
- Upgrading Information
- SonicWall Support

About SonicOS 6.5.0.2-37-158 for NS$_v$ Series

SonicOS 6.5.0.2-37-158 for NS*v* Series is a maintenance release for SonicWall NS*v* Series virtual firewalls. It is available as an SWI file for update to an existing virtual firewall and as an OVA file for a fresh install.

The SonicWall NS*v* Series is SonicWall's virtualized next-generation firewall series which provides Deep Packet Inspection (DPI) security and segmentation in virtual environments. Initially supported on VMware ESXi, SonicOS running on the NS*v* Series offers the same feature functionality and security features of a physical appliance, with comparable performance. SonicOS for NS*v* Series is a fully featured 64-bit SonicOS powered by SonicCore.

SonicOS 6.5.0.2 for NS*v* Series provides almost all features supported on SonicWall hardware platforms running SonicOS 6.5.0. See the *SonicWall NSv Series Getting Started Guide* for information about specific feature support, and the *SonicOS 6.5 for NSv Series* administration documentation and online help for detailed feature information. Documentation is available on the Support portal at https://www.sonicwall.com/en-us/support/technical-documentation by selecting **NS*v* Series** from the **Select A Product** list.

Supported Platforms

SonicOS 6.5.0.2-37-158 for NSv Series is supported on the following SonicWall virtual firewalls:

- NSv 10
- NSv 25
- NSv 50
- NSv 100
- NSv 200
- NSv 300
- NSv 400
- NSv 800
- NSv 1600

Resolved Issues

This section describes the resolved issue in this release. Both the SWI and OVA files include the resolved issue.

Resolved Issues in SWI and OVA

Resolved issue	Issue ID
Adding more than ten Address Objects into an Address Object Group results in the error message, "Status: Error: Address Object in Group: Adding 3.1.1.0 to depth test: Too many objects in group, or too many global group members." Occurs when attempting to add the eleventh Address Object to an AO Group on an NSv 200.	SOSV-2336

Known Issues

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

Known Issues

Known issue	Issue ID
In specific scenarios, booting SonicOS into factory default settings disables the X0 (LAN) IPv4 DHCP lease scope. **Workaround**: Manually enable the default X0 IPv4 DHCP lease scope after the NSv appliance boots up.	SOSV-2125
When **Redistribute remote VPN networks** is enabled from **Network > Routing > OSPFv2**, RIP redistributes the default route even after disabling **Originate Default Route**. **Workaround**: Disable and re-enable RIP.	SOSV-2087
A configured static DHCPv6 scope on the firewall does not work without a dynamic DHCPv6 scope enabled for the same prefix. Clients cannot get a static DHCPv6 lease. **Workaround**: Configure and enable a dynamic DHCPv6 scope for the same prefix.	SOSV-2010
A configured DHCPv6 local server does not send DHCPv6 generic options to a DHCPv6 client.	SOSV-2009
In a Stateful HA pair, dynamic ARP entries are not synchronized to the idle unit.	SOSV-1954
The DHCPv6 local server fails to respond to DHCPv6 relay packets.	SOSV-1933
When DHCPv6 mode is changed from manual to automatic, the client does not send an RS message as expected, but waits until the next RA message comes from the router.	SOSV-1927
NTLM user authentication fails for the first time when the **Redirect the browser to this appliance via the interface IP address** option is enabled, but subsequent logins succeed.	SOSV-1896

System Compatibility

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

GMS Support

SonicWall Global Management System (GMS) 8.4 or higher is required for management of SonicWall NS*v* Series virtual firewalls running SonicOS 6.5.0.2 for NS*v* Series.

Browser Support

SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS 6.5.0.2-37-158 for NS*v* Series. 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 SonicOS system administration.

Product Licensing

SonicWall NS*v* Series virtual firewalls 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

You can download the SWI and OVA files for this release from MySonicWall. For information about obtaining the latest SonicOS image, upgrading the image on your SonicWall NS*v*, and importing configuration settings from another NS*v*, see the *SonicOS 6.5 NSv Series 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.

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. Select the language based on your geographic location to see the EUPA that applies to your region.

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: 6/19/18

232-004412-00 Rev A