

SonicWall SonicOS 6.5.4.v for NSv Series Release Notes

July 2024

This release notes provide information about the SonicWall SonicOS 6.5.4.v-21s-RC2457 for NSv Series release on all NSv platforms.

Topics:

- [About SonicOS 6.5.4.v for NSv Series](#)
- [Supported Platforms](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [System Compatibility](#)
- [Product Licensing](#)
- [Upgrading Information](#)
- [SonicWall Support](#)

About SonicOS 6.5.4.v for NSv Series

SonicOS 6.5.4.v-21s-RC2457 for NSv Series resolves a number of issues found in previous SonicOS releases for the NSv Series virtual firewalls. For details, see the [Resolved Issues](#) section. For deployment requirements and recommendations, see the section.

❗ **IMPORTANT:** For NSv Series on Azure and NSv Series on AWS, version 7.0 is the default deployment on Marketplace. To deploy an NSv running version 6.5.4 on Azure or AWS, use an ARM template deployment instead of deploying from Marketplace.

Refer to the SonicWall NSv 6.5.4 Getting Started Guides for detailed instructions:

<https://www.sonicwall.com/techdocs/pdf/nsv-series-on-azure-6-5-4-getting-started-guide.pdf>

<https://www.sonicwall.com/techdocs/pdf/nsv-series-on-aws-6-5-4-getting-started-guide.pdf>

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

SonicOS 6.5.4.v for NSv Series supports almost all features supported on SonicWall hardware platforms running SonicOS 6.5.4. Refer to the *SonicOS 6.5.4 for NSv Series About SonicOS* administration guide and the appropriate NSv *Getting Started Guide* for information about specific feature support. Also refer to the *SonicOS*

6.5.4 for NSv Series administration documentation set. Documentation is available on the Technical Documentation portal at <https://www.sonicwall.com/support/technical-documentation> by selecting **NSv Series**.

Supported Platforms

SonicOS 6.5.4.v for NSv Series is supported on the following SonicWall virtual firewalls:

VMware ESXi, Hyper-V, and KVM Supported Platforms

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

Azure Supported Platforms

• NSv 200	• NSv 800
• NSv 400	• NSv 1600

AWS and AWS-PAYG Supported Platforms

• NSv 200	• NSv 800
• NSv 400	• NSv 1600

Resolved Issues

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

Issue ID	Issue Description
SOSV-5600	CFS block is not working when TLS hybridized kyber support is default-enabled on Chrome.
SOSV-5599	Heap-based buffer overflow vulnerability in SonicOS IPSec (SNWLID-2024-0012)
SOSV-5550	Firewall reboots when 2FA is enabled for the SSLVPN users.

Known Issues

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

Issue ID	Issue Description
SOSV-5593	The version of NetExtender for Windows included in SonicOS 6.5.4v is not the latest released version. Workaround: Manually download the latest NetExtender version from MSW and then manually update the NetExtender version.
SOSV-5588	The SSL VPN zip file, which includes all SSL VPN client files, has not been updated with the latest versions of the clients. Workaround: Instead, you can download the latest version of the VPN clients from VPN Clients .
SOSV-5586	AWS NSv deployment through AWS CloudFormation template with new VPC will fail at the step EipAssociation .
SOSV-5544	Failed to reset password through Azure portal page
SOSV-5522	After unbinding the TOTP Code for imported LDAP user or domain user, when client logs in, it is not redirecting to new TOTP authentication page.

System Compatibility

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

GMS / NSM Support

The following SonicWall GMS or NSM releases are required for management of SonicWall NSv Series virtual firewalls running SonicOS 6.5.4.v.

- SonicWall Global Management System (GMS On-Premise) 8.7 Service Pack 1 (8.7.1) or higher
- SonicWall Network Security Manager (NSM) 2.3.2 or higher

Browser Support

SonicWall recommends using the latest Chrome, Firefox, Microsoft Edge, or Safari browsers for administration of SonicOS 6.5.4.v for NSv Series. This release supports the following web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher

- Microsoft Edge
- Safari 10.0 and higher running on Mac systems

① | **NOTE:** On Windows systems, Safari is not supported for SonicOS management.

① | **NOTE:** Mobile device browsers are not recommended for SonicOS system administration.

Product Licensing

SonicWall NSv Series virtual firewalls must be registered on MySonicWall to enable full functionality and to receive 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 upgrading the image on your SonicWall NSv virtual firewall, refer to the [SonicOS 6.5 NSv Series Upgrade Guide](#).

① | **IMPORTANT:** For NSv Series on All Platforms:

- For NSv deployments running a previous version of SonicOS 6.5.4.v, upgrading via the **System Update** option in the NSv management console is recommended for this release. The **System Update** option updates both SonicOS and SonicCore to the latest version. For more information and instructions, refer to the [SonicOS 6.5 NSv Series Upgrade Guide](#).
- To obtain the resolution for issues with SonicCore dependency, a fresh installation or **System Update** is needed.

① | **IMPORTANT:** For NSv Series on Azure and NSv Series on AWS, version 7.0 is the default deployment on Marketplace. To deploy an NSv running version 6.5.4 on Azure or AWS, use an ARM template deployment instead of deploying from Marketplace.

Refer to the SonicWall NSv 6.5.4 Getting Started Guides for detailed instructions:

<https://www.sonicwall.com/techdocs/pdf/nsv-series-on-azure-6-5-4-getting-started-guide.pdf>

<https://www.sonicwall.com/techdocs/pdf/nsv-series-on-aws-6-5-4-getting-started-guide.pdf>

For NSv Series on VMware ESXi:

- For NSv deployments running SonicOS 6.5.0.v, a fresh deployment using the OVA file is required to obtain this update.
- This SonicOS 6.5.4.v release is available as an SWI file for SonicOS update on an existing virtual firewall and as an OVA file for a fresh install or **System Update**. You can download the SWI and OVA files from [MySonicWall](#).
- For System Update and fresh deployments, you can download the OVA file from [MySonicWall](#).
- SWI upgrade to this SonicOS 6.5.4.v release is only supported for existing NSv Series on VMware ESXi deployments running SonicOS 6.5.4.v-44v-14-653 or higher.

For NSv Series on Hyper-V:

- This SonicOS 6.5.4.v release is available as an SWI file for SonicOS update on an existing virtual firewall and as a VHD file for a fresh install. You can download the SWI file and a ZIP file containing the VHD file from [MySonicWall](#).
- For **System Update** and fresh deployments, you can download a ZIP file containing the VHD file from [MySonicWall](#).
- SWI upgrade to this SonicOS 6.5.4.v release is only supported for existing NSv Series on Hyper-V deployments running 6.5.4.v-44v-14-676 or higher.

For NSv Series on KVM:

- This SonicOS 6.5.4.v release is available as an SWI file for SonicOS update on an existing KVM virtual firewall and as an IMG file for a fresh install. You can download the SWI and IMG files from [MySonicWall](#).
- For **System Update** and fresh deployments, you can download the IMG file from [MySonicWall](#).
- SWI upgrade to this SonicOS 6.5.4.v release is only supported for existing NSv Series on KVM deployments running 6.5.4.v-44v-14-676 or higher.

For NSv Series on Azure or AWS:

- This SonicOS 6.5.4.v release is available as an SWI file for SonicOS update on an existing virtual firewall running 6.5.4.v-44v-14-676 or higher.
- For a fresh deployment of this SonicOS 6.5.4.v for NSv Series on Azure, go to the Microsoft Azure Marketplace at <https://azuremarketplace.microsoft.com/en-us/marketplace/> and then search for **SonicWallINSv**.
- For a fresh deployment of this SonicWall 6.5.4.v for NSv Series on AWS, go to the Amazon Marketplace at <https://aws.amazon.com/marketplace/search/results?searchTerms=sonicwall+nsv>.

For High Availability deployments (VMware ESXi, Hyper-V, and KVM only):

- HA Stateful Synchronization is supported, which means that the secondary unit will automatically synchronize with the primary unit when SonicOS is updated on the primary.
- When upgrading a High Availability pair using **System Update**, each unit must be upgraded individually. For more information about System Update, refer to the *SonicOS 6.5 NSv Series Upgrade Guide*.
- For a detailed HA upgrade procedure, refer to the *SonicOS 6.5 NSv Series Upgrade Guide*.

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 <https://mysonicwall.com>
- 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>.

About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOS Release Notes
Updated - July 2024
Software Version - 6.5.4.v
232-005813-00 Rev H

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall 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 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 reserves the right to make changes to specifications and product descriptions at any time without notice. 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>.