SonicWall Network Security Manager 2.5 On-Premises

Release Notes

These release notes provide information about the SonicWall Network Security Manager (NSM) 2.5 On-premises release.

Versions:

- Version 2.5.0-HF1 On-Premises
- Version 2.5.0 On-Premises

Version 2.5.0-HF1 On-Premises

October 2024

Important

- Refer to the knowledge base article, How to Upgrade SonicCore and NSM in Closed Network for detailed instructions on upgrading NSM in closed network environment.
- Refer to the knowledge base article, Upgrade NSM on-prem via System Update for detailed instructions on a system upgrade. Prior to update, you need to create a system backup of the NSM on-premises system in case you need to roll back to the prior version. Refer to Backup and Restore an NSM On-Prem System for detailed instructions.
- Refer to knowledge base article, How to Upgrade On-Prem Network Security Manager firmware for detailed instructions on upgrading NSM firmware using SWI files.
- NSM On-Prem supports importing backup file of size upto 30 GB. To keep backup file size in control we recommend to delete device firmware image used for upgrading individual firewalls from Home > Firewalls > Inventory > Action > Upgrade firmware upgrade.

Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.
- **Capacity Requirements:** The capacity requirements for an NSM On-Premises deployment have changed:

Platform	Platform Details	Number of Firewalls	Recommended Configuration
VMware	Supported versions:	1-500	4 Cores, 24 GB RAM
	ESXi 7.0, 8.0	500-3000	8 Cores, 48 GB RAM
Hyper-V	Windows 2019, 2022	1-500	4 Cores, 24 GB RAM
		500-3000	8 Cores, 48 GB RAM
KVM	Linux Kernel 5.15 LTS	1-500	4 Cores, 24 GB RAM
		500-3000	8 Cores, 48 GB RAM
Azure	Standard_D4_v2	1-500	8 Cores, 28 GiB RAM
	Standard_D5_v2	500-3000	16 Cores, 56 GiB RAM

- **Upgrade Instructions:**

  NSM can be upgraded on platforms VMWare, Hyper-V, KVM and Azure using system update or .swi image. You must be at the correct version of NSM before upgrading to NSM 2.5.0-HF1. Refer to the table below before attempting to upgrade to NSM 2.5.0-HF1.

Current Build	Upgrade Path to 2.5.0-HF1
2.4.4-R7	2.4.4-R7 > 2.5.0 > 2.5.0-HF1
2.5.0	2.5.0 > 2.5.0-HF1

What's New

- This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Description
NSM-26192	Option to export CSR in Firewall View is missing(Gen7).
NSM-26120	2FA Users are logged out of NSM when accessing Firewall View(Session Expired error).

Known Issues

There are no known issues for this release.

Additional References

There are no additional references for this release.

Version 2.5.0 On-Premises

September 2024

Important

- Refer to the knowledge base article, How to Upgrade SonicCore and NSM in Closed Network for detailed instructions on upgrading NSM in closed network environment.
- Refer to the knowledge base article, Upgrade NSM on-prem via System Update for detailed instructions on a system upgrade. Prior to update, you need to create a system backup of the NSM on-premises system in case you need to roll back to the prior version. Refer to Backup and Restore an NSM On-Prem System for detailed instructions.
- Refer to knowledge base article, How to Upgrade On-Prem Network Security Manager firmware for detailed instructions on upgrading NSM firmware using SWI files.
- NSM On-Prem supports importing backup file of size upto 30 GB. To keep backup file size in control we recommend to delete device firmware image used for upgrading individual firewalls from Home > Firewalls > Inventory > Action > Upgrade firmware upgrade.
- For customers who update to NSM on-premises 2.5.0 version will be subject to a default backup retention limit of 10. The subsequent day, at 1 AM, solely the 10 backups that have been recently created will be preserved, while the remainder will be automatically deleted. Customers are advised to download or SCP the backups to a remote server, other than the 10 most recent ones, if they wish to preserve it.

Compatibility and Installation Notes

- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- A MySonicWall account is required.

- **Capacity Requirements:** The capacity requirements for an NSM On-Premises deployment have changed:

Platform	Platform Details	Number of Firewalls	Recommended Configuration
VMware	Supported versions: ESXi 7.0, 8.0	1-500 500-3000	4 Cores, 24 GB RAM 8 Cores, 48 GB RAM
Hyper-V	Windows 2019, 2022	1-500 500-3000	4 Cores, 24 GB RAM 8 Cores, 48 GB RAM
KVM	Linux Kernel 5.15 LTS	1-500 500-3000	4 Cores, 24 GB RAM 8 Cores, 48 GB RAM
Azure	Standard_D4_v2 Standard_D5_v2	1-500 500-3000	8 Cores, 28 GiB RAM 16 Cores, 56 GiB RAM

- **Upgrade Instructions:**

  NSM can be upgraded on platforms VMWare, Hyper-V, KVM and Azure using system update or .swi image. You must be at the correct version of NSM before upgrading to NSM 2.5.0. Refer to the table below before attempting to upgrade to NSM 2.5.0.

Current Build	Upgrade Path to 2.5.0
NSM 2.4.0-R32	2.4.0-R32 > 2.4.4-R7 > 2.5.0
NSM 2.4.4-R4	2.4.4-R4 > 2.4.4-R7 > 2.5.0
2.4.4-R7	2.4.4-R7 > 2.5.0

What's New

- **Integration with Cloud Secure Edge:** NSM 2.5.0 supports SonicOS 7.1.2 firmware version. SonicOS 7.1.2 provides Cloud Secure Edge (CSE) Connector integration to enable zero-trust network access to the private applications hosted behind the firewall. NSM users will be able to enable CES connectors from both firewall views and by using templates.
- **Storage Settings in Templates:** NSM now supports firewall storage settings in templates. This feature will help admins configure storage settings in multiple devices through templates.
- **Zero Touch 2.0:** NSM 2.5.0 has enhanced zero-touch capabilities. Zero touch 2.0 is based on a new microservices-based architecture that simplifies the on-boarding of firewalls and establishes reliable connectivity between NSM and firewalls.

- **NSM Backup Enhancements:** There are several enhancements in NSM backup:
    - Starting NSM 2.5.0, users will have an option to specify number of NSM backups they want to retain in the NSM disk. This functionality will enable users to optimize the NSM disk usage. Default number of backups that can be retained by NSM is 10. The minimum number of backup that can be retained in 1 and the maximum is 15.
    - The maximum size of the backup file that can be uploaded to NSM On-Prem via web interface has been raised from 20 gigabytes to 30 gigabytes.
    - NSM "First Setup Wizard" is enhanced to configure SCP location used for copying backup file.
- **Mandatory Change of Default Password:** NSM will present a force password change screen for super-admin logging in with the default password.
- **Change in Default Backup Schedule:** The default schedule has been changed from weekly to bi-weekly.
- **Breadcrumb Changes for NSM HA vs Firewall HA:** Breadcrumb has been changed in the interface to differentiate between NSM HA and Firewall HA.

Resolved Issues

Issue ID	Description
NSM-25575	Certificate import to NSM fails with error "Failed to decode the file contents".
NSM-25401	Unable to register new On-Prem NSM instance using closed network file and displays error that GUID do not match.
NSM-25248	Unable to delete uploaded firewall firmware images for error "deletion failed: Could not find the firmware file based on the software id and current tenant".
NSM-25204	NSM Swagger API page does not load properly and displays error "No operations defined in spec!".

Known Issues

Issue ID	Description
NSM-25798	Manual sync should not be required while manually adding the secondary active HA firewall in NSM.
NSM-25606	NSM 2.4.0 > 2.4.4-R7 SWI upgrade in normal mode throws a 'No response' error in HyperV 2019. Workaround: Please upgrade NSM using online system update mechanism (i.e core roller).
NSM-25603	SWI upgrade is showing 'Not a valid key in the file' error. Workaround: Please upgrade NSM using online system update mechanism (i.e core roller).

Issue ID	Description
NSM-25550	Schedule backup > Backup list page tool tip is showing wrong information when it's in a HA pair.
NSM-25431	System > Firmware Upgrade > Import/Export Settings: "Request failed status code 400" error is observed while trying to restore the settings.

Additional References

NSM-25247, NSM-24878, NSM-24191, NSM-23535, NSM-7126.

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.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

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

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

ⓘ | **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.**

Network Security Manager Release Notes
Updated - October 2024
232-006171-00 Rev B

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.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to “SonicWall Inc.”, to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035