



SonicWall Network Security Manager 2.4

Release Notes

These release notes provide information about the SonicWall Network Security Manager (NSM) 2.4 release.

Versions:

- [Version 2.4.7](#)
- [Version 2.4.6](#)
- [Version 2.4.5](#)
- [Version 2.4.4](#)
- [Version 2.4.3](#)
- [Version 2.4.2](#)
- [Version 2.4.1](#)
- [Version 2.4.0](#)

Version 2.4.7

June 2024

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.
- Refer to [Network Security Manager for OnPrem and SAAS- System Requirements](#) for the latest information on hardware requirements, operating systems, and browser levels.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Description
NSM-24561	NSM Monitor > Log Download Rule for Web Activities is displaying 0 for approximate number of records.
NSM-24505	Scheduled reports are not sent during the configured Schedule Time randomly.
NSM-24449	One firewall is unable to re-acquire into NSM SaaS.
NSM-24379	Live Report > Multicore data is missing for May 10 and May 18 dates.

Known Issues

Issue ID	Description
NSM-24833	CTA report fails with error "Valid PDF download link is not found in CTA Response".
NSM-24560	NSM Analytics data CSV export is displaying "Last Updated" column incorrectly as "_lastTs".
NSM-24545	NSM Group level firmware upgrade is failing with error about bad filename extension.
NSM-23845	Getting 'context canceled' error when doing firewall firmware upgrade using NSM.
NSM-23323	There are issues in NSM Custom report search filter.

Additional References

There are no additional references for this release.

Version 2.4.6

June 2024

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.

- Refer to [Network Security Manager for OnPrem and SAAS- System Requirements](#) for the latest information on hardware requirements, operating systems, and browser levels.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Description
NSM-23667	App control Copilot is missing for Gen 6 devices and templates.

Known Issues

Issue ID	Description
NSM-23845	Getting 'context canceled' error when doing firewall firmware upgrade using NSM.
NSM-23820	Unable to sort the Routing rules from NSM based on the Column "AUTO-ADD ACCESS RULE".
NSM-23708	Firewall status goes to Offline and Unmanaged shortly after a successful sync from NSM.
NSM-23323	NSM custom report search filter issues.

Additional References

There are no additional references for this release.

Version 2.4.5

May 2024

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.
- Refer to [Network Security Manager for OnPrem and SAAS- System Requirements](#) for the latest information on hardware requirements, operating systems, and browser levels.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Description
NSM-23930	Unable to sync or get the firewall back as online and managed.
NSM-23909	Unable to send scheduled report to multiple email addresses.
NSM-23856	Unable to modify a VPN policy that contains a variable for firewall SN on the IKE ID within a template.
NSM-23840	Unable to deploy the static route for tunnel interface using NSM template.
NSM-23685	Incorrect data displayed on NSM firewall address objects list.
NSM-23558	Screens with large number of configurations are not being displayed.

Known Issues

There are no known issue for this release.

Additional References

NSM-23866

Version 2.4.4

May 2024

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.
- Refer to [Network Security Manager for OnPrem and SAAS- System Requirements](#) for the latest information on hardware requirements, operating systems, and browser levels.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Description
NSM-23731	VPN policies page does not load and gets error "Maximum call stack size exceeded", caused by nested Group Object.
NSM-23681	Spyware report shows entries as "Unknown".
NSM-23668	Unable to update / modify DHCP Server Lease Scopes where the Domain Name begins with a numeric character.
NSM-23630	Access Rule Policy is displaying the incorrect Geo-IP Allow/Block Country list.
NSM-23563	NSM Firewall Monitor>Log Download>Rules is displaying incorrect month on custom rule.
NSM-23515	Template - Unable to see virtual interfaces on IP Helper policy in the "From" dropdown.

Known Issues

Issue ID	Issue Description
NSM-23820	Not able to sort the Routing rules from NSM based on the column "AUTO-ADD ACCESS RULE".
NSM-23685	Incorrect data displayed on NSM firewall address objects list.

Additional References

NSM-23651, NSM-23559.

Version 2.4.3

May 2024

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.
- Refer to [Network Security Manager for OnPrem and SAAS- System Requirements](#) for the latest information on hardware requirements, operating systems, and browser levels.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Description
NSM-23595	Spyware report is not showing for most firewalls, in customers tenant, for the last 90 days.
NSM-23593	Scheduled reports are not sent during the configured Schedule Time.
NSM-23592	Firewall is not showing all Botnet data after NSM SaaS 2.4.2 upgrade.
NSM-23536	When data is drilled down in Botnet report, sources tabs shows "No data" for few of the Botnet IPs.
NSM-23476	Filtered Reports show data in NSM but not in the exported scheduled reports.
NSM-23475	Golden Template objects fail with "Schema validation error: property 'range' redefined" error message.
NSM-23406	No statistics / hitcount is shown on NAT rule page.
NSM-23277	User is deleted from MSW but still showing up in NSM SaaS.

Known Issues

Issue ID	Issue Description
NSM-23731	VPN policies page does not load and gets error "Maximum call stack size exceeded", caused by nested Group Object.
NSM-23681	Spyware report shows entries as "Unknown".
NSM-23668	Unable to update / modify DHCP Server Lease Scopes where the Domain Name begins with a numeric character.
NSM-23667	App control Copilot(3441 ID) is missing for Gen6 devices and templates.
NSM-23630	Access Rule Policy is displaying the incorrect Geo-IP Allow/Block Country list.
NSM-23563	NSM Firewall Monitor>Log Download>Rules is displaying incorrect month on custom rule.
NSM-23515	Template - Unable to see virtual interfaces on IP Helper policy in the "From" dropdown.

Additional References

NSM-23665, NSM-23546, NSM-23516, NSM-23470.

Version 2.4.2

April 2024

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.
- Refer to [Network Security Manager for OnPrem and SAAS- System Requirements](#) for the latest information on hardware requirements, operating systems, and browser levels.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Description
NSM-23368	No data error is seen when drilling down on existing Analytics entries.
NSM-23090	Data usage section under Live Reports shows no data for ingress.
NSM-23089	Scheduled reports are not sent during the configured Schedule Time randomly.
NSM-23061	Live Report is not showing data prior to March 6th.
NSM-23037	When Live Report is selected for 7 days or 30 days, it only show data for the last 3 days.
NSM-23003	Dynamic Objects are not available for policy creation within templates.
NSM-22938	Commit for adding syslog server fails with error "schema validation error: property enabled cant be empty value".
NSM-22935	Drilldown data in Botnet reports comes up with "No data" error.
NSM-22782	Received error when accessing Firewall View > Device > High Availability > Settings, "Cannot read properties of undefined (reading 'options')".
NSM-22778	Reports are not loading for some devices.
NSM-22558	Geo-IP filter shows disabled on access rule in NSM firewall view, when it is enabled on the actual firewall.
NSM-22435	Analytics is not showing data for 5 min until 30 mins.
NSM-22407	Products are showing expired on the NSM portal.
NSM-20793	Device > Settings > Storage > Files > Diagnostic Data: Downloading larger file fails with 504 error.

Known Issues

Issue ID	Issue Description
NSM-23323	NSM Custom report search filter issues.

Additional References

NSM-23400, NSM-22226.

Version 2.4.1

March 2024

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.
- Refer to [Network Security Manager for OnPrem and SAAS- System Requirements](#) for the latest information on hardware requirements, operating systems, and browser levels.

What's New

This maintenance release provides fixes for previously reported issues.

Resolved Issues

Issue ID	Description
NSM-22769	Received error when accessing IPSec VPN > Rules and Settings, "Cannot read properties of undefined (reading 'toUpperCase')".
NSM-22599	Security services related alerts stopped getting triggered after NSM 2.4.0 release.
NSM-22591	Drilling down on entries listed as "Unknown" results in no data error.
NSM-22568	Unable to edit backup schedule and getting error "Malformatted Response of [post]".
NSM-22566	Session logs show initiator and responder data transferred values set as NaN TB for some connections.
NSM-22413	Web Activity logs are missing in NSM Analytics for dates 1/11 - 1/20.
NSM-22381	Botnet Reports are not showing any data in NSM.
NSM-22288	False alarm of VPN tunnel status as down in NSM.
NSM-22213	Unable to use template to set Geo-IP.
NSM-22209	NSM "Viruses" report is showing the incorrect name for some signatures as compared to the Firewall.
NSM-22178	No data is available for device with with 7-day essential license
NSM-22151	Geo-IP Filter>Diagnostics>Lookup IP throws error.

Issue ID	Description
NSM-22140	App Control is missing Applications for GEN7 devices within Templates
NSM-22040	Attempt to add exclusion group for CATP fails with error, "Command 'exclude address for-capture-atp name "atp group"' does not match".
NSM-21990	Live Monitor/Reports are not working following RMA of HA unit and report migration.
NSM-21565	Firewall in NSM showing up as "SERIALNUMBER".
NSM-21428	Customer Unable to delete VPN topology in NSM SaaS.

Known Issues

Issue ID	Issue Description
NSM-22782	Received error when accessing Firewall View > Device > High Availability > Settings, "Cannot read properties of undefined (reading 'options')".
NSM-22577	NSM is displaying the wrong default Service object for Filter based DNS policy resulting commit failure of the policy.
NSM-22558	Geo-IP filter shows disabled on access rule in NSM firewall view, when it is enabled on the actual firewall.
NSM-22435	Analytics is not showing data for 5 min until 30 mins.
NSM-22407	Products are showing expired on the NSM portal.

Additional References

NSM-22861, NSM-22803, NSM-22781, NSM-22598, NSM-22575, NSM-22557, NSM-22548, NSM-22497, NSM-22332, NSM-22203, NSM-22058, NSM-21864, NSM-21464.

Version 2.4.0

January 2024

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.

- Refer to [Network Security Manager for OnPrem and SAAS- System Requirements](#) for the latest information on hardware requirements, operating systems, and browser levels.

What's New

- NSM 2.4.0 SaaS brings the support for SonicOS 7.1.1 features in both template and firewall view in NSM. SonicOS 7.1.1 contains the following major features:
 - **DNS Filtering:** DNS security service inspects the DNS traffic in real time and provides an ability to block threats before they reach the network.
 - **Content Filtering (CFS) 5.0:** Content filtering blocks users from loading questionable websites or network resources and restricts the user access to certain types of content on the internet. Customers can use DNS Filtering feature to block, allow, and/or track visits to certain websites and network resources.
 - **NAC support:** NAC ability provide visibility, device profiling, policy enforcement, and access management. Customers can exercise granular control on policy enforcement on the devices connecting to their network
- An option to download access rules from NSM in CSV format is added for better visibility and manageability.
- NSM productivity reports now support CFS 5.0 categories at tenant/group level.
- Auto-firmware upgrade feature in SonicOS 7.1.1 is disabled in both firewall view and template view in NSM since single/group firmware upgrades can be done through the inventory page in NSM.
- GMS will not support SonicOS 7.1.1 features.

Resolved Issues

Issue ID	Description
NSM-22301	Missing data in on-demand 20+day dashboard/details scheduled flow reports.
NSM-22300	NSM Advanced reports are incomplete.
NSM-22041	Details>Sources/Destinations/Source Locations/Destination Locations reports do not load when filtering for 24+ hours in NSM.
NSM-22039	Drilling down into session logs results in "No data" due to 504 Gateway Timeout.
NSM-21765	NAT policy search criteria is not maintained when other filters or views are applied.
NSM-21564	Difference in App signatures between NSM and Individual Firewall.
NSM-21396	Hit counts for CFS rules is not visible in firewall view of NSM.
NSM-21385	The commit push for VPN policy update shows successful in NSM but policy is not updated on firewall.
NSM-20624	Unable to disable firewall static route probes using NSM.
NSM-20622	NSM doesn't gray out disabled static routes.

Issue ID	Description
NSM-19137	CFS blocked total count under Report>Details does not match analytics session logs total count.
NSM-17503	Data mismatch in CTA report under application report and NSM UI.
NSM-15088	Web activity alert & website analytics report does not display information related to connection.
NSM-14943	Date picker for firmware upgrade not working in safari
NSM-10899	BWM not showing up in template for interface configuration.

Known Issues

Issue ID	Issue Description
NSM-22213	Unable to use template to set Geo-IP.
NSM-22151	Geo-IP Filter>Diagnostics>Lookup IP throws error.
NSM-22138	Data missing for random time slots for specific firewall.
NSM-22040	Attempt to add exclusion group for CATP fails with error.
NSM-21990	Live Monitor/Reports are not working following RMA of HA unit and report migration.
NSM-21549	Not able to deploy certificate from NSM.

Additional References

NSM-22212, NSM-22120, NSM-20003.

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

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.

Network Security Manager Release Notes
Updated - June 2024
232-006109-00 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>.

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