SonicWall Network Security Manager 2.3 On-Premises

Release Notes

These release notes provide information about the SonicWall Network Security Manager (NSM) 2.3 On-premises release.

Versions:

Version 2.3.5-1 On-Premises

December 2023

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.
- Customers running NSM version 2.3.4-6-R15 should first upgrade to 2.3.4-6-R17 by mandatorily following steps mentioned in https://www.sonicwall.com/support/knowledge-base/taking-backup-of-nsm-on-premise-before-upgrade/230628174823577/.
- Customers running NSM version 2.3.4-6-R16 should upgrade to 2.3.4-6-R17 using SWI upgrade.
- In user creation workflow, NSM allows specifying primary and secondary emails. Users can login into NSM using username, primary email id or secondary email id. However going forward, in feature releases of NSM, we will be removing secondary emails from user creation workflows. Which means there will not be an option to specify secondary email id while creating new user and existing user will not be able to login using secondary email id. In case you are using secondary email id for login please plan to create another NSM user with same email id so you can continue using secondary email for login after secondary email id support is removed from future releases of NSM.
- NSM On-Prem supports importing backup file of size upto 18 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 6.7, 7.0	500-3000	8 Cores, 48 GB RAM
Hyper-V	Windows 2016	1-500	4 Cores, 24 GB RAM
		500-3000	8 Cores, 48 GB RAM
KVM	Linux Kernal 2.6.17	1-500	4 Cores, 24 GB RAM
	or above	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 using system update or .swi image. The minimum version requirements for upgrading to NSM 2.3.5-1 are:

Platform	Minimum Required Version
VMWare, Hyper-V, KVM, Azure	2.3.4-6-R16

What's New

- This release introduce workflow to reset super admin password.
- While configuring NSM backup, user has ability to specify scp password.
- User can export NSM backup from safemode and scp NSM backup file generated by on-demand backup.
- New user configuration provides ability to select all tenants.
- NSM can generate alert notification based on HA status.

Resolved Issues

Issue ID	Description
NSM-21385	VPN Policy update commit push shows successful in NSM but the configuration is not updated on firewall.
NSM-21341	System > Settings > Administration > Web Management tab is showing error "Unexpected token 'U', "Updated th"... is not valid JSON", while updating the certificate from the certificate drop down.
NSM-21027	NSM On-Prem initial setup Wizard does not change the password.
NSM-21025	NSM On-Prem HA Virtual IP not being used on Active Server.
NSM-19605	HA secondary units are being added to inventory.
NSM-19515	Scheduled Backups are not received on SCP server.
NSM-19486	Analytics Summary reports is not showing correct data. Applications report, Threats, Sources, etc show the same data.
NSM-18900	Switch to Firewall Context View doesn't work for GEN 6 devices. NSM is using wrong Certificate.
NSM-18892	Error received when editing NAT policy "node not found".
NSM-16059	Switch to Firewall Context is very slow for GEN 6 units on NSM system with many firewall.

Known Issues

Issue ID	Description
NSM-21419	Importing large backup file in Schedule Backup is showing error " Request failed with status code 413".

Additional References

NSM-21339, NSM-20845, NSM-20718, NSM-20129, NSM-19586, NSM-19228, NSM-16575, NSM-16574, NSM-7386.

Version 2.3.4-6-R17 On-Premises

October 2023

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.
- Customers running NSM version 2.3.4-6-R15 should first upgrade to 2.3.4-6-R17 by mandatorily following steps mentioned in https://www.sonicwall.com/support/knowledge-base/taking-backup-of-nsm-on-premise-before-upgrade/230628174823577/.
- Customers running NSM version 2.3.4-6-R16 should upgrade to 2.3.4-6-R17 using SWI 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: ESXi 6.7, 7.0	1-500 500-3000	4 Cores, 24 GB RAM 8 Cores, 48 GB RAM
Hyper-V	Windows 2016	1-500 500-3000	4 Cores, 24 GB RAM 8 Cores, 48 GB RAM
KVM	Linux Kernal 2.6.17 or above	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:** The minimum version requirements for upgrading to NSM 2.3.4-6-R17 are:

Platform	Minimum Required Version
VMWare, Hyper-V, KVM, Azure	2.3.4-1-R15

What's New

- This maintenance release addresses issues related to NSM On-Prem Analytics integration, friendly name, vulnerability and other critical issues.

Resolved Issues

Issue ID	Description
NSM-20288	Analytics integration after 2.3.4-6-R16 upgrade does not load any report data.
NSM-20251	HA secondary units are being added to inventory.
NSM-19813	OpenSSH and MariaDB Version Upgrade: Use of vulnerable third-party component.
NSM-19409	NSM updated the Friendly Name in MSW for many managed firewalls.
NSM-19104	When integrating Analytics data, the reports fail to load if Analytics has a complex password.
NSM-18970	In NSM the live reports were blank when Firewall > Monitor > Live Monitor was selected. Confirmed the data displayed in Analytics.
SOC-3151	NSM WebUI does not come up after restoring the backup.

Issue ID	Description
SOC-3150	Restore backup fails because of a script error.
SOC-3147	Upload backup fails for large .enc files.
SOC-3141	NSM On-prem safemode webUI does not update to reflect the state of restore operation.

Known Issues

Issue ID	Description
NSM-19515	Scheduled backups were not received on the SCP server.
NSM-18753	Created a new address object and added it to any group, but got the error **node not found**.
SOC-3159	UI timeout error while restoring backup from safemode.

Additional References

NSM-20621, NSM-20523, NSM-20129, NSM-19886, NSM-19778, NSM-19388.

Version 2.3.4-6-R16 On-Premises

July 2023

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.
- Before upgrading from 2.3.4-6-R15 to 2.3.4-6-R16 it is mandatory to follow recommendation mentioned in https://www.sonicwall.com/support/knowledge-base/taking-backup-of-nsm-on-premise-before-upgrade/230628174823577/.

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 6.7, 7.0	1-500 500-3000	4 Cores, 24 GB RAM 8 Cores, 48 GB RAM
Hyper-V	Windows 2016	1-500 500-3000	4 Cores, 24 GB RAM 8 Cores, 48 GB RAM
KVM	Linux Kernal 2.6.17 or above	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:** The minimum version requirements for upgrading to NSM 2.3.4-6-R16 are:
  - Upgrade using **System Update** and .swi image:

Platform	Minimum Required Version
VMWare, Hyper-V, KVM	2.3.4-1

What's New

- Customers already on Azure, running NSM 2.3.3-5 can export NSM settings and import them in a fresh installation of NSM 2.3.4-6.
- NSM On-Premises has backup improvements that provide a fix for problems which may cause backups to be incomplete or get corrupted.

Resolved Issues

Issue ID	Description
NSM-19213	The web user interface does not load the post-2.3.4-6 upgrade.
NSM-18945	A download of the TSR/Log fails for **Unknown Reason**.

Issue ID	Description
NSM-18941	An upgrade fails for an on-premises NSM running on Azure.
NSM-18521	After navigating to **Policies -> Access Rules** page, an alert is displayed with message **Cannot read properties of undefined (reading 'trackBwEnabled')**.
NSM-18518	Error received when editing NAT policy: **node not found**.

Known Issues

Issue ID	Description
NSM-19740	If you login to an NSM on-premises system after navigating from the Home to the System option, this error is displayed: **Unexpected end of JSON input**.
NSM-19515	Scheduled backups were not received on the SCP server.
NSM-19486	Summary reports are not showing correct data when integrating Analytics into NSM. All Summary reports, such as Applications/Sources/Threats, are showing the same data.
NSM-19409	NSM updated the Friendly Name in MSW for many managed firewalls.
NSM-19104	When integrating Analytics data, the reports fail to load if Analytics has a complex password.
NSM-18970	In NSM the live reports were blank when **Firewall > Monitor > Live Monitor** was selected. Confirmed the data displayed in Analytics.
NSM-18753	Created a new address object and added it to any group, but got the error **node not found**.
NSM-17439	**Unknown Reason** error pops up while doing a swi upgrade using NSM user interface. Word around: Manually reboot NSM to finish the upgrade process.

Version 2.3.4-6 On-Premises

April 2023

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.

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 6.5, 6.7, 7.0	500-3000	8 Cores, 48 GB RAM
Hyper-V	Windows 2016	1-500	4 Cores, 24 GB RAM
		500-3000	8 Cores, 48 GB RAM
KVM	Linux Kernal 2.6.17 or above	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:** The minimum version requirements for upgrading to NSM 2.3.4-6 are as follows:
  - **Upgrading using System Update:**

Platform	Minimum Required Version
VMWare, Hyper-V, KVM	2.3.3-6
Azure	2.3.4-1

What's New

- NSM 2.3.4-6 On-Prem supports source and destination address variables in the SD-WAN topology. This will provide flexibility and scalability in creating SD-WAN rules involving different site locations with unique addresses.
- NSM 2.3.4-6 On-Prem has new RBAC controls. These controls allow administrators to restrict or to allow

the access to 'Schedule Backups' and 'Analytics Agents' screens in NSM.

- Support for ESXi 6.5 is removed for NSM 2.3.4-6.

Resolved Issues

Issue ID	Description
NSM-17814	Upgrades to NSM are reverting the settings back to a previous state.
NSM-17617	Every time a firewall lost WAN connection, an email alert is sent.
NSM-17479	NSM Logs and Alerts/Events got error message every 10 seconds.
NSM-17320	Search does not return results for matched value in service column of access rules.
NSM-17316	Manual device acquisition failed.
NSM-17315	Issue with NSM on-prem deployment where firewall names are showing as the serial number and not the friendly name set on mysonicwall.com.
NSM-17306	Firewall view > Service object shows blank page after NSM upgrade.
NSM-17230	Creating a new address object and adding it to any group throwing error "node not found".
NSM-17194	ZT Device acquisition is failing after installing NSM 2.3.4-1-R11-H1.
NSM-17099	App control commits are failing with schema validation error.
NSM-16989	Unable to delete address objects from NSM management.
NSM-16980	Unable to edit the X0 ip address from NSM.
NSM-16960	Attempting to migrate unit to a new tenant results in error.
NSM-16865	Unable to export NSM settings.
NSM-16821	Firmware upload/reboot fails when pushed from NSM on-prem.
NSM-16819	When creating a Report Rule from firewall view and when saving the report rule, the Delivery Interval gets changed to Daily.
NSM-16818	Creating a Report Rule from firewall view with Delivery Type only being Email fails with error.
NSM-16756	Every user, irrespective of the right given, can download system backups.
NSM-16566	Editing a security policy in the template shows server error.
NSM-16402	Several errors when we try to configure internal wireless for SOHO250W.
NSM-16313	Friendly Name is blank or incorrect (listed as serial) at random times.
NSM-13908	Device status remains online even after device is powered off.

Known Issues

Issue ID	Description
NSM-18284	Under the process monitor 'systemEventsManager' is displayed and shows as stopped.
NSM-18251	When deleting firewall access rules following error "Cannot read properties of undefined (reading 'response')".
NSM-18128	After migrating firewalls from ZT to instant connect, then applying Golden Template created by customers firewall setting, we are getting error.
NSM-18039	Error received when attempting to delete a route.
NSM-17439	Swi upgrade : 'Unknown Reason' error while doing swi upgrade using NSM UI.
NSM-16059	Switch to firewall context is very slow for GEN6 units on NSM system with many firewalls (over 100).
NSM-15692	NSM and analytics integrations shows "No data", if the administrator password of analytics has a % sign in it.

Additional References

NSM-17313, NSM- 17063, NSM-17041, NSM-16852, NSM-16794, NSM-16784, NSM-16780, NSM-16644.

Version 2.3.4-1 On-Premises

November 2022

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.

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.
- **Upgrade Instructions:** The minimum version requirements for upgrading to NSM 2.3.4-1 are as follows:
    - **Upgrading using System Update:**

Platform	Minimum Required Version
VMWare, Hyper-V, KVM	2.3.3-5

What's New

- Ability to upgrade NSM On-Prem from NSM using .swi file under System > Settings > Firmware and Settings page. Please follow the instructions here for upgrade.
- Ability to modify the packet monitor configurations inside the firewall view.
- Ability to reset an NSM On-Prem appliance to factory defaults from NSM under System > Settings > Firmware and Settings page.
- Ability to reboot NSM On-Prem in SafeMode from NSM under System > Settings > Shutdown/Reboot page.
- NSM 2.3.4-1 On-Prem is now integrated with an analytics tool to collect anonymized data to understand the user interactions with NSM workflows better and improve the product by delivering relevant new features using this data. Administrators will see a consent box to opt in/out of this feature on logging into NSM where they can enable the “Allow NSM to collect anonymized usage data” button to opt in. They can always enable or disable this option from the User Profile page at any time.

Resolved Issues

Issue ID	Description
NSM-15917	Unable to export/import settings file from NSM On-Prem.
NSM-15876	NSM On-Prem HA Syncronization Issue: Force syncronization removes the firewall from the Primary NSM.
NSM-15737	Unable to export NSM settings.
NSM-15736	Change from standalone to HA causes firewalls disappear and errors appear on various pages.
NSM-15275	GEN6 access rules MAC and FQDN objects are displayed improperly.
NSM-15044	Unable to access NSM after upgrading to latest version 2.3.3-5-R674 via console.

Issue ID	Description
NSM-14694	Wrong application IDs used in NSM templates.
NSM-14692	Unable to update Enforce password complexity.
NSM-14682	Errors received when updating local user - 'email_address is empty'. Password has length greater than MAX_LEN '64'.
NSM-14656	Creating a schedule report fails with an error "there was an error while saving the report rule".
NSM-14530	Unable to SSH to console after upgrading to 2.3.3-4.
NSM-14513	Cannot sort DHCP and ARP leases by search or vendor for GEN7 devices on NSM.
NSM-14512	NSM feature "Whitelist Login IP Addresses" does not block user access to NSM tenant.
NSM-14448	Not able to enable “Ignore DF(Don't Fragment) Bit” in Template/IP Sec/Advanced.
NSM-13949	NSM shows HA disabled with no serial number of standby unit but HA is enabled on firewall.
NSM-13942	ITF - GEN7 firmware upgrades are failing in On-Prem 2.3.3-4.
NSM-11394	Certificate Service Request (CSR) generated in NSM is invalid.
NSM-9327	Firewall view is not showing all the IPS signatures that are actually showing in the firewall interface.

Known Issues

Issue ID	Description
NSM-16402	There are several errors when trying to configure internal wireless for SOHO250W.
NSM-16313	Friendly name is blank or incorrect (listed as serial) at random times.
NSM-16059	Switch to Firewall Context is very slow for GEN6 units on NSM system with many firewall (over 100).
NSM-13908	Device status remains online even after device is powered off.
NSM-13727	NSM not displaying correct admin name.

Additional References

NSM-16339, NSM-16338, NSM-15724, NSM-15366, NSM-12622, NSM-11582.

Version 2.3.3-6 On-Premises

July 2022

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.

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 6.5, 6.7, 7.0	500-3000	8 Cores, 48 GB RAM
Hyper-V	Windows 2016	1-500	4 Cores, 24 GB RAM
		500-3000	8 Cores, 48 GB RAM
KVM	Linux Kernal 2.6.17 or above	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 requirements:** The minimum version requirements for upgrading to NSM 2.3.3-6 are as follows:
  - **Upgrading using System Update:**

Platform	Minimum Required Version
VMWare, Hyper-V, KVM	2.3.2-R12-H4

  - **Upgrading using .swi Image:**

Platform	Minimum Required Version
VMWare, Hyper-V, KVM	2.3.3-5-R674

What's New

- Ability to upgrade NSM On-Prem using the SWI file in safemode. Please follow the upgrade instructions in the Getting Started Guide. This is the only supported way of upgrading NSM On-Prem offline using the SWI file.
- Ability to reset an NSM on-premises appliance to factory defaults via the NSM Management Console.
- The following configurations are now exported as a part of Golden Template from a device:
  - ARP
  - DHCP server
  - Network monitor
  - SD-WAN
  - Gateway anti-virus signatures
  - Anti-spyware signatures
  - Intrusion prevention signatures
  - App control signatures
  - Default service-objects, service-groups and schedules.
  - Route policies
- Validations are added for variables for interface settings in templates so that an error occurs when an invalid input is entered.
- A new "Firmware upgrade progress bar" is added in the Upgrade Firmware wizard for admins to track the status of a firmware upgrade for a device.

Resolved Issues

Issue ID	Description
NSM-14808	Unable to access management interface after enabling zero touch on NSM.

Issue ID	Description
NSM-14611	Restoring from scheduled/on-demand backup is failing due to invalid backup file.
NSM-14609	Unable to configure HA settings on NSM On-Prem.
NSM-14568	Can't enable management or user protocols on X1 WAN when mode is set to DHCP.
NSM-14407	Unable to export NSM settings.
NSM-14378	Group name is changed but it is not taking effect in inventory view.
NSM-14330	Unable to see drooms application in template view.
NSM-14211	Device Licenses: Duplicate entries are seen in NSM secondary.
NSM-14185	Commit for online/managed firewall is stuck in deploying due to process killed.
NSM-14184	Certificates are not in sync in NSM HA.
NSM-14182	Interface performance is very poor since upgrading to On-Prem 2.3.3-4-R18.
NSM-14144	Adding management interface to template failed with an error "Please enter a valid interface name".
NSM-14074	Unable to set email ID with a .tech. NSM is only taking .com.
NSM-14048	Test' SCP settings gives 'Success' result for any random input.
NSM-14046	Commit and deploy is going to scheduled state.
NSM-14035	Switch to firewall context view doesn't work for Gen 6 devices.
NSM-13998	Display error or notification when configuring CFS URI object.
NSM-13989	Data out of bounds error is displayed intermittently while trying to update radius information using template.
NSM-13886	15k devices is slow to load NAT policies page and gets error message "No Response".
NSM-13885	Unable to modify templates as an error message is displayed "NSM appears busy with other configuration operations. Please try again later".
NSM-13873	Firewall view does not show correct MTU value.
NSM-13871	NSM showing incorrect Geo-IP location.
NSM-13745	DNS is lost after system update upgrade. This results in no serial/license in NSM.
NSM-13735	Template was applied on the firewalls even when they are unchecked.
NSM-13720	Unable to set management when DHCP is selected.
NSM-13701	GEN7 firmware upgrade is not working through NSM On-Prem.
NSM-13693	Service group is not showing the right setting.
NSM-13175	AppFlow server IP change cannot be saved in template.
NSM-13151	Secondary HA firewall is being added to inventory once secondary becomes active.
NSM-13103	In template/app control, enabling "Block" and "Log" is not displayed in the interface.
NSM-12975	Internal error message shows while trying to push ip helper policy using golden template.

Issue ID	Description
NSM-12595	NSM is creating commits for units that are not in the group in which a template is applied.
NSM-11311	Packet capture is not configurable in "Switch to Firewall Context".
NSM-10711	App control issues in template.

Known Issues

Issue ID	Description
NSM-14656	Creating a schedule report fails with an error "there was an error while saving the report rule".
NSM-14530	Unable to SSH to console after upgrading to 2.3.3-4.
NSM-14155	NSM is not pushing license to secondary firewall for existing firewall HA setup.
NSM-13908	Device status remains online even after device is powered off.
NSM-13727	NSM is not displaying correct admin name.
NSM-11394	Certificate service request(CSR) generated in NSM is invalid.
NSM-9327	Firewall view is not showing all the IPS signatures that are actually showing in the firewall interface.
NSM-7277	Wireless dashboard is missing information.
NSM-7126	Fails to acquire HA pair when secondary unit is active.

Additional References

NSM-14377, NSM-13582, NSM-13581.

Version 2.3.3-5 On-Premises

May 2022

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.

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.
- 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 6.5, 6.7, 7.0	500-3000	8 Cores, 48 GB RAM
Hyper-V	Windows 2016	1-500	4 Cores, 24 GB RAM
		500-3000	8 Cores, 48 GB RAM
KVM	Linux Kernal 2.6.17 or above	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

What's New

- **NSM System Backup:** Administrators can now schedule a NSM system backup to recover last known good state from a failure.

Resolved Issues

Issue ID	Description
NSM-13204	Serial number is not displayed on breadcrumb after registration.
NSM-12991	Delete icon is missing for uploaded firmware.
NSM-12928	Unable to acquire gen 7 firewall due to connection reset by peer.
NSM-12902	Firewall update fails with error "Failed to update the firewall".
NSM-12119	Virtual IP does not switch to the active node after force fail-over.

Known Issues

Issue ID	Description
NSM-14048	'Test' SCP settings gives 'Success' result for any random input.
NSM-14035	Switch to firewall context view doesn't work for Gen 6 devices.
NSM-14032	Interface accepts invalid file format on 'Import Backup'.
NSM-13885	Unable to modify templates. Error message is displayed as "NSM appears busy with other configuration operations. Please try again later."
NSM-13745	DNS is lost after system upgrade. This results in no serial/license number being applied to the server in NSM.
NSM-13727	NSM is not displaying correct administrator name.
NSM-13151	Secondary high availability firewall is being added to inventory once secondary becomes active.
NSM-13103	In TemplateView > App Control, enabling "Block" and "Log" information is not displayed.
NSM-8502	Cannot configure vlan over wire mode. Also, paired interface is not showing in SDWAN orchestrator.
NSM-8225	After failover to secondary, the device shows down in the inventory (Issue is reproducible on license reset / factory reset of the device).
NSM-7277	Wireless dashboard has missing information.

Version 2.3.3-4 On-Premises

March 2022

Important

- NSM On-Prem 2.3.3-4 upgrade image is currently not available. You can either do a fresh installation or a perform a system upgrade. Refer to the knowledge base article, Upgrade NSM on-prem via System Update for detailed instructions on a system upgrade.
- Prior to update, 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.
- With this release, the number of devices for scheduled TSR and EXP backups is not limited. Administrators can run a backup on demand or create weekly or monthly backup schedules.

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.
- The capacity requirements for an NSM On-Premises deployment have changed:

Platform	Platform Detials	Number of Firewalls	Recommended Configuration
VMware	Supported versions:	1-500	4 Cores, 24 GB RAM
	ESXi 6.5, 6.7, 7.0	500-3000	8 Cores, 48 GB RAM
Hyper-V	Windows 2016	1-500	4 Cores, 24 GB RAM
		500-3000	8 Cores, 48 GB RAM
KVM	Linux Kernal 2.6.17 or above	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

What's New

- **Template Enhancements:**
  - When a new interface is created, the default address object for that interface is created automatically.
  - When an existing interface is edited, the related address object for that interface is automatically updated.
  - Zone creation in templates creates the zone subnets address group.
  - Variable support is extended to configuring routing rules and for setting up the ethernet address in static range configuration under DHCP server lease scopes.
  - When a new device is added to an auto-commit-enabled device group that has a template with variables previously applied to it, a resolve variables option is presented for the new device (NSM-10116).
  - Firewall's fail-over and LB setting configuration is supported in the templates.
  - Validation checks have been built in so an error is shown if an incorrect IP address is entered.
- **New Filters on the Commits Page:**
  - Four new filters have been added on the **Commit** page under operational status: Pending Approval, Approval Overdue, Approved and Rejected.

- **Login to unit:** Login to unit opens in a new tab in browser.
- **Automatic Commits:** Commits are automatically created for the following operations on the firewall inventory page:
    - Synchronizing licenses at the group level
    - Flushing ARP cache
    - Rebooting at the group level

Resolved Issues

Issue ID	Description
NSM-12816	The user is logged out of NSM once an LTU is performed on a Gen 7 device.
NSM-12648	Importing a certificate for web management settings gives the following error: **X-DEVICE-ID header is not provided or is invalid**.
NSM-12569	Increase TSR download timeout value.
NSM-12473	Commit fails to disable auto generated rules on the Zone configuration made in Template configuration.
NSM-12421	NSM pushes a template with SMTP server for automation, and the password did not push over correctly.
NSM-12419	Editing an IPv6 access rule results in an error: **object access_rules ipv4 does not exist**.
NSM-12366	NSM shows differences when no changes have been made to unit since it last synchronized.
NSM-12339	When adding DHCP scope using pre-pop interface and DNS Proxy is enabled, DNS server entries are limited to 1.
NSM-12337	Unable to login to NSM because the response to Get command for [https://IP-address/api/manager/system/licenses/isNSMRegistered] returned a status code of 500.
NSM-12322	NSM HA is not auto synchronized.
NSM-12318	NSM does not push signatures to firewall when NSM and firewall both are in closed network.
NSM-12308	Cannot sort any column on the ARP page on GEN6 and GEN7 firewalls when added to NSM from NSM portal.
NSM-12174	Cannot enable Botnet Filter on new or existing access rules.
NSM-12173	When creating a Multipath route using multiple Tunnel Interfaces and adding the second path, the gateway is not grayed out when interface is selected as Tunnel Interface.
NSM-12144	**Firewall > Network > System > Interfaces** page does not correctly display the WAN interface added to the Failover & LB group.
NSM-12091	Static DHCP entry is not correctly assigning DNS settings.

Issue ID	Description
NSM-11982	The App Rule and CFS rule creation not working from session logs.
NSM-11827	**Storage** shows up twice in the left pane in the **Firewall View**.
NSM-11826	**VAP Object** and **VAP Profile** cannot be edited in the **Firewall View**.
NSM-11808	Multiple template issues on Geo-IP Filter page.
NSM-11717	Unable to increase the Virtual AP client limit only for SOHO250W through NSM.
NSM-11659	API response for zones has wrong properties key.
NSM-11650	The error: **t.commits is undefined** indicates a configuration difference between NSM and the firewall.
NSM-11641	User authentication **failed for index 1 out of bounds for length 1** for NSM On-Premises Radius.
NSM-11618	NSM **Firewall View** does not show correct MTU value.
NSM-11588	Message **Index of the interface.: interface with the same name already exist** appears when modifying VTI through NSM.
NSM-11512	Not able to edit security action profile from NSM.
NSM-11469	Address object update is failing with invalid argument error.
NSM-11459	NSM losing device status time to time.
NSM-11371	Applying Template config creates Commit & Deploy in Global Default tenant and not custom tenant with workaround.
NSM-11361	Browsing to **VPN Topology > Global Settings** creates a permanent template.
NSM-10917	Multiple issues on the **Diagnostics** page.
NSM-10904	Acknowledging or deleting Alerts does not update until screen is refreshed.
NSM-10703	Slow UI when On-Premises NSM loads 2000 Firewalls.
NSM-10602	Incorrect error messages for NSM registration errors.
NSM-10508	Error on access rule priority change.
NSM-10458	NSM not booting into Safe Mode.
NSM-10359	GUIDs are not matching in KVM Console and NSM GUID.
NSM-9665	Unable to download logs.
NSM-9399	Fails to reliably auto Sync settings while performing a force-failover.
NSM-8838	Unable to export NSM configuration from On-Premises -NSM portal.
NSM-8791	Disabled ZT and changed ports and cannot re-enable.
NSM-8688	Moving manually acquired device between tenants requires you to input the password again.
NSM-8355	Acquisition fails when the exp of the firewall > 20MB.
NSM-8186	Wrong status when secondary in active state is switched off from ESXi.
NSM-7162	HTTPS port is not configurable in NSM; both firewall and template affected.
NSM-6413	**Purge All** is not working.

Issue ID	Description
NSM-6326	VPN green light is missing on several VPNs that are up.
NSM-5550	SSL VPN shows incorrect group routes.

Known Issues

Issue ID	Issue Description
NSM-13465	NSM firewall goes through long CPU spikes which make the interface unresponsive for 5 to 10 minutes due to multiple post request every 3 minutes.
NSM-13175	AppFlow Server IP change cannot be saved in the template.
NSM-13151	Secondary HA firewall is being added to Inventory once Secondary becomes Active.
NSM-13103	The interface doesn't display any enabled features of an application which is configured in NSM template. For example, when **Block** and **Log** is enabled for BACKUP-APPS application, the interface did not display.
NSM-13084	After applying the golden template, changes which require a restart don’t show the **Restart Required** message in NSM anywhere.
NSM-13061	The golden template failed to apply access rule updates to the Gen 6 firewall.
NSM-13056	Not able to set probe with tunnel interface on custom route.
NSM-12975	CFS profile allowed URLs failed to get handled when using golden template.
NSM-12971	Must specify an explicit gateway when using main mode error while trying to push group VPN setting using golden template.
NSM-12965	Internal error message displayed while trying to push IP helper policy using golden template.
NSM-12137	Device status remains online even after device is powered off.
NSM-11394	Certificate Service Request (CSR) generated in NSM is invalid
NSM-11265	Unable to acquire HA firewall when secondary firewall is active.
NSM-10509	Network topology is not displaying.
NSM-9327	Firewall view is not showing all the IPS signatures that are actually visible in the firewall interface.
NSM-7277	Login to Unit - Wireless Dashboard missing information.

Additional References

The following ticket numbers indicate resolved tickets that were opened by customers:

NSM-12506, NSM-12340, NSM-12335, NSM-12327, NSM-12305, NSM-11691, NSM-11418

Version 2.3.2-Hotfix 4 On-Premises

March 2022

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 either the on-premises or SaaS Network Security Manager Getting Started Guide for the latest information on hardware requirements, operating systems, and browser levels.
- NSM On-Prem 2.3.2-R12-H4 upgrade image is currently not available. You can either do a fresh install or a system upgrade. See Upgrade NSM on-prem via System Update for detailed instructions on a system upgrade.

Resolved Issues

Issue ID	Description
NSM-13145	Unable to access NSM Web-UI on a custom port after system update.
NSM-12495	Gen7 acquisition fails with error: "Wrong file: mismatch between product SFID=6 and file SFID=3".
NSM-12477	Unable to setup HA using NSM due to the following error: "High Availability cannot be enabled as association failed".
NSM-12464	GUIDs in KVM console are not matching with NSM GUID.
NSM-12458	NSM HA settings are not synchronized even after doing forced synchronization.
NSM-12444	Gen7 acquisition fails with error: "Wrong file: mismatch between product SFID=6 and file SFID=3".
NSM-12320	When there is no pending task on Secondary Active NSM, NSM busy error is continuously displayed.
NSM-12319	NSM HA unit setting up wrong ip for NSM on firewall.
NSM-12184	Unit acquisition fails with error: "MONGO no documents in result".
NSM-12043	Unable to export logs from NSM.
NSM-12035	Version column of Inventory page does not show current device firmware information.
NSM-11977	Inventory "Search" function is not working after upgrade from 2.3.1 to 2.3.2.
NSM-10910	NSM is inaccessible, Login issue with error: "Unknown Reason".

Known Issues

Issue ID	Issue Description
NSM-12863	Device is going to unmanageable state after fail over to secondary. Force sync throws error "Device serial no. doesn't match".
NSM-12856	KVM - Auto sync not happening after force fail over.
NSM-12845	IP address, if changed before configuring HA, not reflected under HA Settings page.
NSM-12818	GAV does not populate signatures in NSM after uploading "All Required" file, UI throws error "Cannot read properties of undefined (reading '0')".
NSM-12679	Unable to add new firewall to Secondary Active NSM.
NSM-12667	When HA is tried disable, the HA process crash.
NSM-12665	NSM logs out as soon as you click on System > Users option.
NSM-12566	NSM using more Memory.
NSM-12514	Under certain scenarios, Virtual IP redirects to Standby NSM.
NSM-12507	Settings which are changed are not being reflected after the Primary is turned off and turned back on with Secondary (Active).
NSM-12300	NSM HA management port does not sycn between Primary and Secondary NSM.
NSM-12298	With NSM deployed in no DHCP environment, IP is not fetched unless NSM is restarted the very first time before HA configuration.

Version 2.3.2-Hotfix 3 On-Premises

January 2022

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 either the on-premises or SaaS Network Security Manager Getting Started Guide for the latest information on hardware requirements, operating systems, and browser levels.

Resolved Issues

Issue ID	Description
NSM-12416	Log4j2 is updated to version 2.17.1 to address CVE-2021-44832.

Version 2.3.2-Hotfix 2 On-Premises

December 2021

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 either the on-premises or SaaS Network Security Manager Getting Started Guide for the latest information on hardware requirements, operating systems, and browser levels.

Resolved Issues

Issue ID	Description
NSM-12280	Logback upgraded to version 1.2.9 to address CVE-2021-42550.
NSM-12232	Log4j is updated to version 2.17.0 to address CVE-2021-45105.

Version 2.3.2-Hotfix 1 On-Premises

December 2021

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 either the on-premises or SaaS Network Security Manager Getting Started Guide for the latest information on hardware requirements, operating systems, and browser levels.

Resolved Issues

Issue ID	Description
NSM-12171	Log4j is updated to version 2.16.0 to address CVE-2021-44228 and CVE-2021-45046.

Version 2.3.2 On-Premises

November 2021

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 either the on-premises or SaaS Network Security Manager Getting Started Guide for the latest information on hardware requirements, operating systems, and browser levels.

What's New

- **CA Certificate Import:** Helps customer to download CA certificate to be able to enable LDAPS for user authentication.

Resolved Issues

Issue ID	Description
NSM-11060	Address Group once created in VPN Wizard doesn't show up in drop down list.
NSM-10922	NSM losing device status time to time.
NSM-10507	Creating custom access rule or editing the existing rule[LAYER ONE NETWORKS LLC] throws the following error: "Source and destination cannot be of different IP version" .

Issue ID	Description
NSM-10289	Zero Touch crashing time to time.
NSM-10288	Unable to export logs from NSM.
NSM-9984	Group action>firmware upgrade for GEN7 devices not working on NSM.
NSM-9782	[Firewalls > Groups] Moving an unit from unassigned to Root group throws the following error in UI: "Device 'NSA 2600 - ZT' (Serial Number: C0EAE4EAB2AE) cannot be migrated from the wrong Device Group (input GroupID=, found GroupID=5eafb08719b21461ccc1cb44)" .
NSM-9566	Error while importing NSM settings to new NSM.
NSM-9373	Login_to_unit GEN6 is not working in Onprem.
NSM-9302	Interface name not displayed on editing a route policy created for VPN tunnel interface[ITF-Systemhaus GmbH].
NSM-9274	Scheduling commit and deploy is not getting scheduled.
NSM-9218	Source address of default HTTPS Mgmt access rule is not displayed correctly after configuring within template.
NSM-8884	Device Administration screen throws the following internal error: "parsing body body from "" failed, because json: cannot unmarshal string into Go struct field AdministrationAdministration.administration.idle_logout_time of type float64".
NSM-8791	When Zero Touch button is disabled, drop-down is still editable and then cannot re-enable the Zero Touch button.
NSM-8786	Template lockout and timeout change fails.
NSM-8560	No entry is getting added even after successful configuration under RBL Filter (Template view) > User Defined SMTP Server List.
NSM-8525	While configuring the route policy the following error is thrown: "interface value is unreasonable.".
NSM-8486	VLan Translation entries are not listed in NSM UI for Gen6 device.
NSM-8445	Restart chassis screen is not available in NSM screen for super massive unit.
NSM-8400	Network > Interface > Add or Edit Interface : Template variable created for Domain Name does not support.
NSM-8285	Add route policy - unable to search dropdown by typing in any field.
NSM-7805	Policy > Rules and Policies > NAT Rules : Editing NAT policy fails with "Command 'no reflexive' does not match" error.
NSM-7306	NSM does not use SSL TLS option even if we configure for Notification.
NSM-7209	Customer cannot test LDAP through on-prem NSM.
NSM-7035	Users imported from LDAP/AD are not correctly displayed for Approval Groups; only User Role is displayed.
NSM-7029	Acquiring UTM through custom port (443) from Zero Touch is not working.
NSM-5886	Delete All throws error "path /api/manager/firewall/sdwan/all-sla-class-objects was not found".

Issue ID	Description
NSM-5195	Clicking 'Save' fails with js error after making config in 'TACACS Users' tab.
NSM-4243	Missing IP validation while creation the VAP profiles.

Known Issues

Issue ID	Issue Description
NSM-11469	Address object update is failing with invalid argument error.
NSM-11445	VPN Wizard pushes incorrect zones for protected networks for Hub and Spoke.
NSM-11371	Applying template config creates commit & deploy in Global Default tenant and not custom tenant with workaround. **Workaround**: Move Firewall from Custom Tenant to Global Default Tenant apply Template and move back to custom tenant.
NSM-11265	Unable to acquire HA firewall when Secondary is active.
NSM-11001	NSM shouldn't limit the number of devices for scheduling backups of TSR and EXP.
NSM-10703	Slow UI when NSM on-prem loads 2000 Firewalls (High cpu usage by browser). **Workaround**: Segregate firewalls with 300 firewall in each Tenant.
NSM-10458	NSM 2.3.1 not booting into safe mode.
NSM-10359	GUIDs are not matching in KVM Console and NSM GUID.
NSM-8502	Cannot configure vlan over wire mode and paired interface is also not showing in SDWAN Orchestrator.
NSM-7898	Closed Network: Gen7 acquisition fails with few errors.
NSM-7162	HTTPS port is not configurable in NSM; both firewall and template are affected.
NSM-3666	Unable to edit the VPN and 4to6 Tunnel Interface under Network > Interfaces.

Additional References

NSM-7599, NSM-4380

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

ⓘ | **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 - December 2023
232-005783-00 Rev V

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