SonicWall SonicOS and SonicOSX 7.0.1
Release Notes

These release notes provide information about the SonicWall SonicOS and SonicOSX 7.0.1 release.

Versions:

Version 7.0.1

April 2021

SonicOS/X 7.0.1 introduces support for the SonicWall NSa 3700 network security appliance. This release provides several new features and enhancements, and fixes a number of issues found in previous releases.

Compatibility and Installation Notes

SonicOS/X 7.0.1 is supported on the following SonicWall network security appliances:

• NSa 2700	• TZ270 / TZ270W	• NSv 270
• NSa 3700	• TZ370 / TZ370W	• NSv 470
	• TZ470 / TZ470W	• NSv 870
• NSsp 15700	• TZ570 / TZ570W	*deployed on any of these platforms:*
	• TZ570P	• AWS (BYOL or PAYG)
	• TZ670	• Microsoft Azure
		• VMware ESXi
		• Microsoft Hyper-V
		• Linux KVM

- SonicWall recommends using the latest Chrome, Firefox, Safari, or Edge browsers for administration of SonicOS/X. Incognito and private mode are not supported.
- A MySonicWall account is required. SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support.
- 4G/LTE devices are supported on SonicWall TZ and NSa Series firewalls. To see a list of supported devices, go to:
  Wireless-cards-and-broadband-devices-supported-on-sonicwall-firewalls-and-access-points
- Network Security Manager (NSM) 2.2 supports management of all SonicWall firewalls running 7.0.1.

What's New

- **Support for Auth Code during SafeMode Authentication**

  You can use the appliance Auth Code as the Maintenance Key when accessing SafeMode on unregistered firewalls running SonicOS 7.0.1. The Auth Code is displayed in the web management interface and on the label affixed to the bottom of the appliance.
- **Switch Integration:**
  - **Native VLAN configuration** support in SonicOS for SonicWall Switches

    Provides ability for administrator to specify which VLANs do not carry a VLAN tag. This helps with SonicWave provisioning.
  - **New Port Description field** for each switch port provides easy labeling of ports
  - **Eight Switches per firewall** are supported, up from four Switches in previous releases
  - **Support for multiple standalone Switches** for SonicWall firewall High Availability deployments
- **SDWAN support on Root Instance** of NSsp15700
- **One-Arm Mode** interface support for NSv private cloud deployments on VMware, Hyper-V and KVM platforms

  In One-Arm Mode, traffic enters and leaves the appliance on the same interface.
- **PPPoE interface mode support** on NSv 270/470/870
- **SR-IOV NIC support** on NSv 270/470/870 deployed on KVM platforms

  The Single Root I/O Virtualization (SR-IOV) PCI standard allows virtual machines to share access to a physical network interface card (NIC) installed in the hypervisor.
- **Bootstrap configuration provisioning support** for NSv 270/470/870 on KVM platforms
- **Firmware upgrade support from NSv 7.0.0** firmware version to NSv 7.0.1 in Policy Mode
- **SonicOS Classic Mode availability on NSv** 270/470/870:
  - Firewall Mode switching available between Classic and Policy Mode
  - Firewall Mode switching option on the NETWORK | Firewall > Advanced page
  - Firewall Mode switching option in MySonicWall controls visibility of this option on the firewall, must be enabled for the NSv serial number in the MySonicWall account
  - Firewall Mode choice of Classic or Policy Mode for new SonicOS/X 7.0.1 NSv deployments
  - Fresh NSv 7.0.1 deployments in Classic Mode support settings imports from NSv 6.5.4.v instances

Resolved Issues

Issue ID	Issue Description
GEN7-9974	On TZ Series platforms, the administrator cannot modify the Account Expires option in a Guest account using time increments expressed in units (Days, Hours, or Minutes) other than the unit used in the original configuration.
GEN7-10226	With Client DPI-SSL enabled, when the SSL client uses ECDHE-ECDSA cipher suites to connect towebsites which support TLS1.3 such as Facebook, the connection cannot be established.

Issue ID	Issue Description
GEN7-10783	On NSv or TZ firewalls, the Audit Log is incorrect or missing information when importing a configuration settings file.
GEN7-12366	On NSv or TZ firewalls, an excluded user setting within a DENY access rule does not work.
GEN7-13697	When using DHCP over VPN on a VLAN interface, if bound to a VLAN interface in unassigned state, the peer cannot decrypt packets.
GEN7-15097	Percentage-Based WAN Load Balancing does not work as expected. Running the traffic flow based on user defined Percentage-Based WAN Load Balancing fails with existing/previous traffic flows.
GEN7-15344	NSsp 15700 does not show Network Monitor Object in Routing rule and Probe drop-down list.
GEN7-15352	When using Single Sign-On on an NSsp 15700, the option for Partition selection is not available when adding an SSO agent.
GEN7-15601	When Single Sign-On is toggled in the SSO Agent, RADIUS accounting packets are consistently dropped by the firewall rule. Because of this, the SSO Agent keeps trying to connect and keeps failing.
GEN7-15646	On NSv series platforms, SSH management of the firewall fails when the SSH port is configured to use a non-standard port.
GEN7-15672	On NSv series platforms, the web management interface hangs after deleting the DoS action profile that is used by a DoS policy.
GEN7-16351	On an NSsp 15700 with Authentication Partitioning enabled, the LDAP server does not have a partition setting. When adding or editing an LDAP server, there is no Partition field or setting.
GEN7-16659	On NSv series platforms, the product code and model name are not displayed in the SonicOS/X web management interface and management console after registration using an NSv serial number if the serial number has never been registered before. If the serial number has been registered by someone (even if this SN has been deregistered), this issue does not occur. Restarting the NSv after registration will also solve this issue.
GEN7-16824	On TZ series platforms, the Prevention and Detection settings for many IPS signatures are not consistent by default with the category settings.
GEN7-17413	On an NSsp 15700 High Availability pair, the standby firewall loses web and console responsiveness when Virtual MAC is disabled on the active firewall with Override MAC Address enabled.
GEN7-17546	On NSsp 15700, FTP packets are dropped when using FTP through a VPN tunnel.
GEN7-17566	On a TZ470 after upgrading firmware, the X8 and X9 interfaces display "NO LINK" and are down.
GEN7-17664	With Client DPI-SSL enabled, changing the re-signing certificate does not take effect without rebooting the firewall.
GEN7-17929	When editing Access Rules on SonicOS 7.0, the Bandwidth Management profiles are set to Disabled by default and the error message, "Error: property 'bandwidth_ management' can't be empty object" is displayed on the first attempt to apply a rule.
GEN7-18021	In a High Availability pair with Enable Stateful Synchronization selected, attempting to use the Tools & Monitors > Active Connections page results in an error popup

Issue ID	Issue Description
	message, "HA idle".
GEN7-18025	When attempting to delete a custom zone that is no longer used in any interface, an error message displays, "Object is in use by an Access Rule."
GEN7-18035	On an NSa 2700, no link is established when connecting a 10 GB SFP+ module on interface X18 to a SonicWall Switch.
GEN7-18097	An NSv for Hyper-V deployed on Windows server 2019 cannot boot up successfully when clicking "factory default" in the management console.
GEN7-18381	The DNS settings cannot be saved when configuring IPv6 options under Specify DNS Servers Manually on the NETWORK | DNS > Settings page.
GEN7-18457	On an NSa 2700 with more than 40,000 Single Sign-On user sessions, the web management interface hangs for about 3 minutes after navigating to the DEVICE | Users > Status page.
GEN7-18553	On an NSa 2700, moving the native bridge mode of an interface to a LAN interface causes a segmentation fault.
GEN7-18562	On a TZ670 with Link Aggregation configured, traffic fails after shutdown of the Parent Interface of a static LAG.
GEN7-18651	On an NSa 2700 with multiple Switches portshielded to the firewall X0 interface and active client connections, traffic flow does not resume after restarting the firewall.
GEN7-18654	On an NSa 2700 with multiple Switches connected, the firewall sometimes goes down when trying to delete Switches.
GEN7-18734	A backed up configuration with X1 in DHCP mode but without an IP address cannot be imported when attempting to reboot the firewall with that saved configuration, resulting in a failed reboot attempt.
GEN7-18775	On an NSa 2700 High Availability pair, toggling Preempt mode on the active firewall causes the standby firewall to reboot.
GEN7-18927	On an NSa 2700, the default management IP address for the MGMT port cannot be changed, and the error message, "Command no one arm mode does not match" is displayed.
GEN7-18958	On an NSa 2700 using the classic navigation view, the PortShield Groups page is missing.
GEN7-19039	An error popup, "Network error", is displayed after exporting configuration settings on a firewall with connected SonicWall Switches and then rebooting with factory defaults and importing the saved settings file, although the settings are successfully imported after some time.
GEN7-19255	On an NSsp 15700, login fails after importing configuration settings that were exported from the same NSsp.
GEN7-19741	An NSa 3700 reboots multiple times and the traffic interface ports go down with "NO LINK" displayed for ports X28 and X29.
GEN7-19767	On an NSv for Azure Active/Standby High Availability deployment, the firmware cannot be upgraded.
GEN7-19886	On NSv series, the WAN interface cannot be configured in PPPoE mode due to the error "Schema validation error: unknown property 'pppoe'".
GEN7-19970	On an NSv AWS PAYG (Pay as you Go) instance, the LAN to WAN traffic cannot be

Issue ID	Issue Description
	matched with the respective LAN to WAN security policy if Gateway AntiVirus is enabled in the action profile before the NSv AWS instance is associated in MySonicWall.
GEN7-20062	Before registering an NSv AWS PAYG instance, Capture Threat Assessment report generation displays an incorrect error message and fails to generate the CTA report.
GEN7-20280	On an NSa 2700, the power button does not work with a long press after using a short press to shut down the system. Short Press takes less than 5 seconds, while Long press needs more than 5 seconds.
GEN7-20315	On an NSa 2700 with more than 40,000 Single Sign-On users, clicking on Users > Status > Show Count results in an unknown error.
GEN7-20316	On an NSa 2700 with more than 40,000 Single Sign-On users, an error is displayed while trying to change Access Rules: "Error: unknown property 'block_traffic_for_ single_sign_on'".
GEN7-20673	The IPv6 Default LB Group of an interface already configured as part of Failover & LB incorrectly allows some settings to still be configurable.
GEN7-20752	High Availability cannot be configured if the standby/peer serial number was once wrongly specified.
GEN7-21397	On NSsp 15700, files transferred using SMB are not sent to Capture ATP for analysis.
GEN7-21398	On NSsp 15700, .zip archive type files are not sent to Capture ATP for analysis.
GEN7-21486	On NSsp 15700, enabling Enhanced Security resulted in no files being sent to the Capture ATP engine.
GEN7-21582	On NSsp 15700, Block Until Verdict does not block malicious file download over HTTP/HTTPS with DPI-SSL enabled.
GEN7-21741	SonicOSX (Policy Mode) does not support the common ‘real-world’ use case where 5-tuple matches multiple security (ULA) policies with differing (but partially overlapping) web categories applied in a positive matching allow action, unless it applies to non-referrer type websites which are rated with one or multiple categories in the applied group.
GEN7-21799	Packets with length larger than 1522 bytes cannot be received when Jumbo Frame is enabled on NSa 2700/3700 firewalls and the interface's MTU has been set to 9000.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-14373, GEN7-15097, GEN7-18103, GEN7-18280, GEN7-18494, GEN7-18585, GEN7-18591, GEN7-18634, GEN7-18666, GEN7-18730, GEN7-18760, GEN7-19009, GEN7-19086, GEN7-19355, GEN7-19384, GEN7-19404, GEN7-19459, GEN7-19460, GEN7-19529, GEN7-19537, GEN7-19546, GEN7-19559, GEN7-19593, GEN7-19606, GEN7-19612, GEN7-19619, GEN7-19649, GEN7-19650, GEN7-19659, GEN7-19721, GEN7-19777, GEN7-19820, GEN7-19830, GEN7-19974, GEN7-20038, GEN7-20050, GEN7-20110, GEN7-20124, GEN7-20204, GEN7-20246, GEN7-20247, GEN7-20366, GEN7-20411, GEN7-20414, GEN7-20510, GEN7-20517, GEN7-20544, GEN7-20601, GEN7-20699, GEN7-20708, GEN7-20766, GEN7-20821, GEN7-20856, GEN7-20866, GEN7-21036, GEN7-21047, GEN7-21069, GEN7-21082, GEN7-21094, GEN7-21225, GEN7-21234, GEN7-21235, GEN7-21236, GEN7-21310, GEN7-21320, GEN7-21321, GEN7-21323, GEN7-

21357, GEN7-21358, GEN7-21360, GEN7-21363, GEN7-21393, GEN7-21400, GEN7-21438, GEN7-21445, GEN7-21464, GEN7-21490, GEN7-21493, GEN7-21555, GEN7-21556, GEN7-21558, GEN7-21592, GEN7-21728, GEN7-21742, GEN7-21771, GEN7-21773, GEN7-21774, GEN7-21880, GEN7-21917, GEN7-22007, GEN7-22055, GEN7-22084, GEN7-22151, GEN7-22194, GEN7-22236, GEN7-22277, GEN7-22353, GEN7-22358, GEN7-22391, GEN7-22423, GEN7-22443, GEN7-22600, GEN7-22652, GEN7-22775, GEN7-22787, GEN7-23040

Known Issues

Issue ID	Issue Description
GEN7-16351	On NSsp with Authentication Partitioning enabled, there is no Partition field or setting when adding or editing an LDAP server.
GEN7-19930	High Availability settings are lost, but other settings are retained when importing configuration settings to an NSa 2700 that were exported from an NSa 2600 running SonicOS 6.5.4.7.
GEN7-21228	A client PC cannot obtain a DHCP IP address in certain deployments involving IP Helper over an unnumbered tunnel VPN. Occurs when an unnumbered tunnel VPN is established between two firewalls, where FW1 is a DHCP server and FW2 has IP Helper enabled, and the client PC is connected to FW1.
GEN7-21977	Adding, deleting and configuring or managing Dell X series switches on an NSa 3700 is not working as expected and the error message, "Error: Index of the Extended Switch Instance" is displayed.
GEN7-22151	During SonicOSX web management, the browser might display the error "Failed to open cache db". This occurs because SonicOSX web management is not supported from browsers in private or incognito mode, including Firefox, Chrome and Edge. **Workaround**: Manage the firewall using a browser in normal mode.
GEN7-22269	An error pops up saying, "Unknown Reason" when accessing the firewall in non-configuration/readonly mode and attempting to select or clear the check box of any option, such as on the Users > Local Users & Groups > Settings page. A more descriptive error message should be displayed.
GEN7-22706	When deploying multi-level Switch daisy chaining, it takes more than five minutes to detect a Switch at the third level. That is, after connecting it to a Switch that is already connected with daisy chaining to a Switch connected to the firewall.
GEN7-22772	The VLANs of the parent Switch are not properly configured on the child Switches in multi-level daisy chaining.
GEN7-22807	Client connections consistently fail with "Timeout" log messages when attempting to connect to a firewall with SSL VPN Server enabled.
GEN7-22950	After registering the firewall using the manual license keyset method and entering the license keyset, the security services Signature File ID (SFID) is incorrect when checked on the POLICY | Security Services > Summary page under UPDATE SIGNATURES MANUALLY.
GEN7-22972	When using SSH Terminal, a LAN PC cannot connect to an SSH session after disabling and then enabling SSH management on the X0 interface.
GEN7-23108	X1 cannot be enabled administratively after an NSv is registered using the manual keyset.

Issue ID	Issue Description
GEN7-23121	On NSsp, Instances sometimes stop working soon after firmware upgrade. This occurs when LDAP is enabled with multiple LDAP servers, due to an issue related to the LDAP referrals. **Workaround**: Disable LDAP referrals in SonicOSX.
GEN7-23131	In a Stateful High Availability deployment, the standby unit sometimes stops working after adding, editing or deleting a CFS Custom Category.
GEN7-23165	On NSv, inbound "Deny" access rules from WAN to WAN for HTTPS Management access sometimes do not block traffic.
GEN7-23211	On NSv, the Protocol tab/screen is not available when editing an interface with Zone set to WAN and Mode / IP Assignment set to PPPoE.

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.

SonicOS and SonicOSX Release Notes
Updated - April 2021
Software Version - 7.0
232-005596-00 Rev B