SonicOS 7.2

Release Notes

These release notes provide information about these SonicWall SonicOS 7.2 releases:

Versions:

Version 7.2-7015

April 2025

This version of SonicOS 7.2 is a feature release for existing platforms and also resolves issues found in previous releases.

Important

- If managing your SonicWall firewalls using Network Security Manager (NSM), do not upgrade your firewalls to SonicOS 7.2 until NSM 3.0 becomes available.
- SonicOS 7.2 is not currently FIPS-compliant or Common Criteria compliance.
- SonicWall firewalls running SonicOS 7.2 cannot be managed using Global Management System (GMS).
- Downgrading to SonicOS 7.0.1 from SonicOS 7.2 is not supported.
- Upgrading SonicOS 7.0.1 to 7.2 for NSv requires a fresh installation of NSv for all platforms. (For more information, refer to NSv upgrade from 7.0.1 to 7.1.X.)
- Use the Firmware Auto Update Feature in SonicOS 7.2 to ensure that your firewall always has the latest updates for critical vulnerabilities. (For more information, refer to Firmware Auto Update.)

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.

Supported Platforms

The platform-specific version for this unified release is the same:

Platform	Firmware Version
TZ Series	7.2-7015
NSa Series	7.2-7015
NSv Series	7.2-7015
NSsp Series	7.2-7015

- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700

- NSv 270
- NSv 470
- NSv 870

- NSsp 10700
- NSsp 11700
- NSsp 13700
- NSsp 15700

SonicOS NSv deployments are supported on the following platforms:

- AWS (BYOL and PAYG)
- Microsoft Azure (BYOL)
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM

What's New

- **SAML 2.0 support for Generation 7 firewalls**

  SonicOS 7.2 provides for SAML-based authentication. See the SonicOS 7.2 SAML Feature Guidefor more information.

- **SonicWall firewalls can act as an NTP server**

  SonicWall Generation 7 firewalls can now be configured to act as NTP servers.

- **Support for WPA2, WPA3, and EAP security protocols**

  WPA2, WPA3, and EAP security protocols are now supported on wireless TZ models running in Station Mode.

- **DNS Proxy Rule Limit Increase**

  The DNS proxy rule limit has been increased to support up to 1,024 entries.

- **New DPS-SSL CA certificate**

  A new SonicWall Firewall DPI-SSL certificate has been added.

Resolved Issues

Issue ID	Issue Description
GEN7-37508	When importing a configuration that has WAN to TrustZone secure WireMode interfaces configured, traffic is not blocked.
GEN7-45207	When a LDAP server with subdomains are added as dynamic LDAP servers, and using LDAP search for a username in the subdomain, the management interface will become unresponsive.
GEN7-47528	When installing NetExtender software from SSLVPN portal page for 32-bit Windows, the message **The installer is only for x64 machine.** is displayed.
GEN7-48392	The error **Remote Reset** is displayed when performing a firewall firmware upgrade using NSM for firewalls configured with High Availability Stateful Synchronization enabled.
GEN7-48431	A network monitor probe fails through a DSLite tunnel when the probe type is set to **PING/TCP**
GEN7-50446	The Setup Guide fails with the error: **Script is missing one or more "exit" command(s)** if **LTE/5G** for the module device type is selected.
GEN7-50853	A failure message is displayed when **Reset counters in routing rules** is selected.
GEN7-50898	Syslog data sent from the firewall are incomplete when SSO is enabled and the zone is a trusted zone.
GEN7-51032	When Wireless LAN is disabled, Wireless Controller Mode is not changed to Non-Wireless.
GEN7-51273	IPv6 ULA redirection is fails to function as expected.
GEN7-51389	Address Object: Netmask is shown incorrectly in the NSM management interface after the **C&D.Network** type with **Network** as `0.0.0.0` and **Prefix** as `255.0.0.0` will be `0.0.0.0` and `255.255.255.255` instead of `0.0.0.0` and `255.0.0.0`.
GEN7-51413	A new SonicWall Firewall DPI-SSL CA certificate has been added.
GEN7-51508	Clicking on 'Open SSH terminal session' intermittently fails.
GEN7-51561	The IPv6 HTTPS server cannot be accessed when Client DPI-SSL is enabled.
GEN7-51603	Local users members of SonicWall Administrators are logged out after two minutes even when actively using the management interface when **Open user's login status window in the same window rather than in a popup** is enabled.
GEN7-51628	The error **ip-assignment is not a reasonable value** is displayed when removing a Port redundancy from the interface. This occurs if the port redundancy was configured in SonicOS 7.0.1-based build and changing the configuration on SonicOS 7.1.1 and later.
GEN7-51697	Numbered VPN tunnel interfaces show incorrectly when getting the interface status (ifOperStatus) using SNMP.

Issue ID	Issue Description
GEN7-51762	The Cloud Secure Edge (CSE) Connector is not available until the **Synchronize** button on the **Device License Registration** page is clicked.
GEN7-51883	Unable to add an FQDN Address object to an Address group that is part of a NAT policy.
GEN7-51903	The Certificate Error **HTTPS handshake SSLv3 alert: certificate unknown** is displayed when accessing HTTPS the Management page.
GEN7-52011	To upgrade the firmware to SonicOS 7.2 on firewalls deployed in High Availability and managed by Network Security Manager (NSM): 1. Disable the **High Availability Stateful Synchronization** option on the High Availability Active firewall. 2. Restart both of the High Availability firewalls. 3. After the firewalls restart and are accessible, ensure that the **High Availability Stateful Synchronization** option is disabled on both of the firewalls. 4. Perform the firmware upgrade to SonicOS 7.2. 5. After both the HA firewalls are upgraded to SonicOS 7.2, enable the **High Availability Stateful Synchronization** option. After the firewalls are upgraded to SonicOS v7.2.0 the next firmware upgrade to a higher version can be done directly from NSM without following the above steps.
GEN7-52180	Unable to add an FQDN Address object to an Address group that is part of a NAT policy.
GEN7-52193	PSIRT Advisory: SNWLID-2025-0001
GEN7-52283	*NSv series only:*, NAT, Route, and SSLVPN settings are missing after upgrading when L3 High Availability IP addresses are configured but L3 High Availability is disabled.
GEN7-52368	NetExtender users see the error **Account Already in Use** when trying to connect to SSL VPN.
GEN7-52462	FQDN address objects cannot be added to FQDN Address Groups if the FQDN Address Group is used in NAT policies.
GEN7-52654	*NSv series only:* cannot be deployed on vCenter 8. the certificate can not verified by Vcenter 8. With this fix there is a tradeoff and special instructions need to be followed for deployment on Vcenter 7. *A Knowledgebase article will be supplied.*
GEN7-52661	The log `Syslog Website Accessed ID 97` is not getting reported in Policy Mode.
GEN7-52176	PSIRT Advisory:SNWLID-2025-0009 (CVE-2025-32818)

Known Issues

Issue ID	Issue Description
GEN7-52544	On the **Access Point Monitor** page, with a wireless client to connected to the Access Point, the client **Allow** and **Deny** buttons are always grayed-out even if the ACL function is enabled or disabled.
GEN7-52611	NAT policy info in the Access Policy log is not shown in the log message when Flow Report is enabled.
GEN7-52723	SAML references are shown in Tech Support Report (TSR) when running in Policy Mode even though it is not supported.
GEN7-52894	An interface that is part of a custom zone with a name that contains special characters shows the zone and mode as being unassigned.
GEN7-52995	The User session option **Open user's login status window in the same window rather than in a popup** does not work for a SAML user if accessing the HTTPS URL directly.
GEN7-53036	The Global VPN Client (GVC) fails to connect when using the NETBIOS format "Domain\username" to connect with the Authentication Partition Domain.
GEN7-53118	For SAML configuration and downloading the XML metadata from an Identity Provider, and then importing this XML file to the firewall, the,firewall will display: **Restart Required!**. After clicking the **Restart** button , only the Identity Provide certificate is saved; the IDP configuration will not be saved. **Workaround:** Save the firewall configuration before restarting the firewall.
GEN7-53128	The **Redirect Authentication** page may Intermittently not display when using SAML with **One Login** or **GSuite IDP** when DPI-SSL is enabled. **Workaround:** Exclude the SAML IDP domains in the DPI-SSL **Common Name** exclusion list.

Additional References

GEN7-48730, GEN7-49240, GEN7-49740, GEN7-50244, GEN7-50367, GEN7-50443, GEN7-50523, GEN7-50550, GEN7-50589, GEN7-50621, GEN7-50638, GEN7-50649, GEN7-50652, GEN7-50694, GEN7-50700, GEN7-50720, GEN7-50732, GEN7-50745, GEN7-50757, GEN7-50758, GEN7-50768, GEN7-50785, GEN7-50809, GEN7-50868, GEN7-50869, GEN7-50874, GEN7-50890, GEN7-50912, GEN7-50924, GEN7-50926, GEN7-50994, GEN7-51031, GEN7-51044, GEN7-51046, GEN7-51099, GEN7-51101, GEN7-51150, GEN7-51159, GEN7-51199, GEN7-51261, GEN7-51286, GEN7-51295, GEN7-51303, GEN7-51312, GEN7-51335, GEN7-51352, GEN7-51393, GEN7-51395, GEN7-51421, GEN7-51445, GEN7-51462, GEN7-51473, GEN7-51488, GEN7-51503, GEN7-51533, GEN7-51550, GEN7-51551, GEN7-51560, GEN7-51619, GEN7-51626, GEN7-51652, GEN7-51663, GEN7-51736, GEN7-51747, GEN7-51775, GEN7-51796, GEN7-51815, GEN7-51830, GEN7-51860, GEN7-51928, GEN7-51931, GEN7-51990, GEN7-52009, GEN7-52025, GEN7-52028, GEN7-52049, GEN7-52052, GEN7-52081, GEN7-52083, GEN7-52152, GEN7-52187, GEN7-52191, GEN7-52221, GEN7-52257, GEN7-52284, GEN7-52340, GEN7-52341, GEN7-52342, GEN7-52349, GEN7-52362,

GEN7-52366, GEN7-52374, GEN7-52381, GEN7-52413, GEN7-52469, GEN7-52474, GEN7-52475, GEN7-52522, GEN7-52525, GEN7-52679, GEN7-52775, GEN7-52852

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.**

SonicOS Release Notes
Updated - April 2025
Software Version - 7.2
232-006322-00 Rev A

Copyright © 2025 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.