

SonicOS 7.1.2 Release Notes

These release notes provide information about these SonicWall SonicOS 7.1.2 releases:

Versions:

- [Version 7.1.2-7019](#)

Version 7.1.2-7019

August 2024

This version of SonicOS 7.1.2 is a feature release for existing platforms and also resolves issues found in previous releases.

Important

- This SonicOS 7.1.2 firmware will not be available on MySonicWall for NSsp 15700. Please contact your Service Account Manager for the firmware.
- If you are managing your firewall using Network Security Manager (NSM), SonicOS 7.1.2 requires NSM 2.5, now available in SaaS. (The on-premises version will be available in September 2024).
- Downgrading to SonicOS 7.0.1 from SonicOS 7.1.2 is not supported.
- Upgrading SonicOS 7.0.1 to 7.1.2 for NSv requires a fresh installation of NSv for all platforms. (For more information, refer to [NSv upgrade from 7.0.1 to 7.1.1.](#))
- Use the Firmware Auto Update Feature in SonicOS 7.1.2 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	7.1.2-7019
NSa Series	7.1.2-7019
NSv Series	7.1.2-7019
NSsp Series	7.1.2-7019

- 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

- **Cloud Secure Edge Connector:** SonicOS now integrates Cloud Secure Edge Connector in SonicOS 7.1.2, allowing remote users to securely access private networks using zero-trust capabilities.

Benefits of the solution

- **Reduced Attack Surface:** Organizations can prevent unauthorized access attempts by adopting a zero-trust approach of “Trust No One, Always Verify,” even if a device is breached in the network perimeter.
- **Simplified Remote Access:** Cloud Secure Edge Connector integration in SonicOS 7.1.2 allows employees to securely access authorized applications from anywhere, on any device, without having to deal with repetitive and complex VPN and Access Policy configurations. With Cloud Secure Edge, all user and device-level access policies are defined in the cloud command center.
- **A Better User Experience:** Enabling ZTNA has never been easier. Secure access can now be enabled with a few clicks and a simple private resource definition on your SonicWall firewall.

① **NOTE:** The Cloud Secure Edge Connector is not available for SonicWall firewalls configured to operate in Policy Mode.

- **Enhancement related to Firewall Storage Module:** This enhancement focuses on improving the robustness of the firewall storage module to ensure the system does not face issues such as errors accessing storage or entering unsolicited Safe Mode.

Resolved Issues

Issue ID	Issue Description
GEN7-33934	When DPI-SSL is enabled, users are unable to send email attachments larger than 1 MB .
GEN7-34484	Audit logs are cleared when the firewall is restarted.
GEN7-39872	Users may get disconnected while downloading a file when using NetExtender.
GEN7-44421	The Update IP Address Dynamically field does not get updated when adding a static ARP entry.
GEN7-44519	When authenticating using NetExtender, and changing an expired AD/LDAP/RADIUS password, this error is displayed: <code>NetExtender was unable to change your password. Server response error.</code> The password in the AD/LDAP/Radius server is changed, but the hint on the client system is incorrect.
GEN7-44690	A SSL-VPN login fails to authenticate when configured for LDAPS and the user tries to authenticate using a Common Access Card (CAC).
GEN7-45194	VPN-based SD-WAN groups are displayed in the drop-down list on the SLA Probes page when they should be excluded.
GEN7-46030	No error is displayed when an incorrect file is uploaded on the Firmware Upload page.
GEN7-46333	Unreadable characters are displayed in some of the events in ArcSight format syslog messages.
GEN7-46338	Bandwidth Management is not working in a App Rule when the action object is selected to use a bandwidth management object.
GEN7-46494	User names and group names are reset to Administrator instead of to their respective user or group names in CFS policies after the firewall restarts.
GEN7-46897	If the Global VPN Client uses an internal DHCP Server and the DHCP over VPN relay IP overlaps with the DHCP scope, when assigning an IP address in a DHCP scope, it may use the relay IP to assign IP addresses, leading to dynamic lease issues.
GEN7-46926	A configuration using AWS displays the error <code>Error: property 'region' expected one of the following options: for these regions: CapeTown, HongKong, Jakarta, Osaka, Milan, Stockholm, and Behrain.</code>
GEN7-47160	User Login Authentication redirection fails on all browsers when using a custom port for HTTPS Management.
GEN7-47173	<i>NSa and NSsp series only:</i> LLDP profiles are missing on the Networking > Switching > L2 Discovery page.
GEN7-47185	<i>NSa and NSsp series only:</i> Local packet mirroring does not work.
GEN7-47327	The Virtual Office web page times out, displaying a blank white screen.

Issue ID	Issue Description
GEN7-47567	App Rules over DPI-SSL are not working when TLS hybridized Kyber support is enabled on Chrome browsers. (This support is now enabled by default on Chrome browsers.)
GEN7-47628	The ability to update microcode using Safe Mode has been added to be used under direction of customer support when needed.
GEN7-47691	Switch VLAN trunking does not work correctly on firewalls with more than 31 interfaces when loading a configuration from 7.0.1 or earlier onto later builds.
GEN7-47736	SSL-VPN licenses are being consumed, preventing users from connecting.
GEN7-47743	Using TLS using a LDAP local certificate with EC curves P-521 is not accepted for FIPS140-3.
GEN7-47756	The login fails when a user with accent characters in their name uses LDAP authentication.
GEN7-47867	When configuring an SD-WAN rule and selecting address objects with "/" in their name displays the error <code>Error: property 'destination' can't be empty object.</code>
GEN7-47953	<i>All TZ models, NSa 2700, and NSa 3700 only:</i> Under some conditions, the core dump storage may grow larger than 500 MB in size.
GEN7-48149	The hardware monitor controller may report occasional false alarms, including fan failures.
GEN7-48173	Two-Factor Authentication via TOTP fails for LDAP and Radius users when using NetExtender.
GEN7-48288	Logging in using Radius using a RSA pin authentication for SSLVPN users fails.
GEN7-48414	When adding a static ARP Entry with colons, it is displayed incorrectly with double colons: <code>xx::xx::xx::xx::xx::xx</code> .
GEN7-48420	Stack-based buffer overflow vulnerability in SonicOS HTTP server (SNWLID-2024-0008)
GEN7-48526	Content Filtering Service (CFS) blocking over DPI-SSL is not working when TLS hybridized Kyber support is enabled on Chrome browsers. (This support is now enabled by default on Chrome browsers).
GEN7-48612	Heap-based buffer overflow vulnerability in SonicOS SSL-VPN (SNWLID-2024-0009)
GEN7-48624	High Core 0 utilization may be experienced when multiple network monitors are configured.
GEN7-48698	Client certificate authentication does not work when using NetExtender unless a local user with same name as in the certificate exists with SSL-VPN services privileges,
GEN7-48705	Users and Groups are showing <code>No data</code> when Authentication Partitioning is enabled.
GEN7-48754	Authentication failures may be experienced when using multiple LDAP servers when Authentication Partitioning is enabled.

Issue ID	Issue Description
GEN7-48755	When importing the users from the AD server, the Email attribute details are not imported, causing users using two-factor authentication to not receive a One-Time-Password by email.
GEN7-48761	When using client certificate authentication, an user is able to log in using a revoked certificate into the management interface, SSL-VPN web portal, and when connecting over SSL-VPN using NetExtender.
GEN7-48958	The SonicWall root certificates store does not contain a GlobalSign Root CA R6 Certificate.
GEN7-48990	When mapping AWS auto-scaled EC2 instances to address groups, the instance name and IP addresses are correctly identified in the Profile Objects AWS page, but the created address objects have the IP address octets reversed.
GEN7-49115	When using DPI-SSL, the block page may not be displayed.
GEN7-49189	Firewall may restart automatically under certain circumstances when using DPI-SSL.
GEN7-49451	<i>NSsp15700 only:</i> The default buffer size for a non-master blade when fetching the Geo-IP map database may experience an overflow if the database size exceeds the maximum limit.
GEN7-49453	A Guest administrator is unable to fully manage guest users.
GEN7-49544	Heap-based buffer overflow vulnerability in SonicOS IPSec (SNWLID-2024-0012)

Known Issues

Issue ID	Issue Description
GEN7-28519	Border Gateway Protocol (BGP) cannot be established when MD5 authentication is enabled.
GEN7-34246	Browser NTLM Authentication functionality is not working. User must log into the firewall in order to authenticate.
GEN7-41593	When upgrading a High Availability pair, if LACP is enabled, then High Availability should be disabled in order to upgrade and each unit must be upgraded individually.
GEN7-43016	NSv deployment displays the error disk image missing when using an <code>.ova</code> file Workaround: <ol style="list-style-type: none"> 1. Unzip the <code>.ova</code> file to three files: <code>vmdk</code> file, <code>nvr</code> file and <code>ovf</code> file. 2. Upload the three files instead of the <code>.ova</code> file.
GEN7-43500	After changing the name of a local user, the entry is still displayed in the Server DPI-SSL Exclusion and Server DPI-SSL Inclusion lists and the user with the changed name cannot be selected.

Issue ID	Issue Description
GEN7-43554	Unable to add valid domains to the Custom Malicious Domain Name list and White List pages after adding an domain one because the pending configuration is still present. Workaround: Logging out and back in should resolve the issue.
GEN7-44642	<i>For NSSP 15700 only:</i> HTTPS Management on X1 is not accessible when the MGMT/Chassis IP and X1/Aux IP are in the same subnet.
GEN7-45252	<i>For NSSP 15700 only:</i> An intermittent issue occurs when the Standby firewall fails to start from uploaded firmware. <code>Wrong firmware to boot</code> is displayed in printed in the command-line interface (CLI) after clicking the restart image with current settings. Workaround: Perform a forced failover of the firewall. The upgrade should now be successful.
GEN7-47528	When installing the NetExtender software from the SSL VPN portal page for 32-bit Windows, the message <code>The installer is only for x64 machine</code> is displayed. Workaround: Download and install the NetExtender software directly from sonicwall.com .
GEN7-49766	Generating a Capture Threat Assessment report fails if the Capture Threat Assessment report is generated using a custom logo that is too large.
GEN7-49782	When making configuration using Cloud Secure Edge > Access Setting , and adding a Private CIDR object under the connector, the zone assignment drop-down does not display all the available zones.
GEN7-49808	When making configuration under Cloud Secure Edge > Access Settings , the management interface displays the error <code>You must associate at least one member object to this group</code> when attempting to delete any address object from the Default CSE Allowed CIDRs group if it contains an FQDN object.

Additional References

GEN7-39938, GEN7-41275, GEN7-41953, GEN7-42134, GEN7-44298, GEN7-45652, GEN7-45701, GEN7-46228, GEN7-46405, GEN7-46482, GEN7-46498, GEN7-46515, GEN7-46611, GEN7-46690, GEN7-46779, GEN7-46780, GEN7-46782, GEN7-46785, GEN7-46829, GEN7-46831, GEN7-46935, GEN7-47261, GEN7-47282, GEN7-47339, GEN7-47406, GEN7-47407, GEN7-47545, GEN7-47546, GEN7-47563, GEN7-47597, GEN7-47630, GEN7-47698, GEN7-47724, GEN7-47725, GEN7-47789, GEN7-47807, GEN7-47809, GEN7-47928, GEN7-47945, GEN7-48003, GEN7-48060, GEN7-48117, GEN7-48164, GEN7-48185, GEN7-48198, GEN7-48228, GEN7-48248, GEN7-48389, GEN7-48390, GEN7-48439, GEN7-48593, GEN7-48602, GEN7-48703, GEN7-48747, GEN7-48790, GEN7-48836, GEN7-48893, GEN7-48969, GEN7-49113, GEN7-49167, GEN7-49209, GEN7-49213, GEN7-49711, GEN7-49789

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.

SonicOS Release Notes
Updated - August 2024
Software Version - 7.1.2
232-006152-00 Rev C

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>.