SonicOS 7.3.0
Release Notes

These release notes provide information about these SonicWall SonicOS 7.3.0 releases:

Versions:

Version 7.3.0-7012

July 2025

This version of SonicOS 7.3.0 is a feature release for existing platforms and also resolves issues found in previous releases.

Important

- SonicOS 7.3.0 is not currently FIPS-compliant or Common Criteria compliance.
- SonicWall firewalls running versions of SonicOS 7.0.*x* or later cannot be managed using Global Management System (GMS).
- Downgrading to SonicOS 7.0.*x*, SonicOS 7.1.*x*, and SonicOS7.2.*x* from SonicOS 7.3.0 is not supported.
- Upgrading SonicOS 7.0.1 to 7.3.0 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 7.3.0 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

- A MySonicWall account is required.
- Network Security Manager (NSM) 3.1 is required to manage firewalls using SonicOS 7.3.0.
- SonicOS 7.3.0 supports NetExtender 10.2.
- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.

Supported Platforms

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

Platform	Firmware Version
TZ Series	7.3.0-7012
NSa Series	7.3.0-7012
NSv Series	7.3.0-7012
NSsp Series	7.3.0-7012

- 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

- **Simultaneous Release of SonicOS and Network Security Manager (NSM)**

  SonicOS 7.3.0 and Network Security Manager 3.1 now release together — ensuring immediate compatibility and a seamless upgrade experience.

- **Automatic installation of critical firmware updates are enabled by default**

  Firewalls can now **automatically upgrade firmware, even under Network Security Manager Network Security Manager** removing manual dependencies and ensuring faster adoption of critical updates.

- **Enhanced Security Defaults (Read this article to learn more.)**
  - **Stronger password complexity** is enforced by default.
  - **Login rate limiting** is enabled by default to prevent brute-force attempts.
  - Ability to **invalidate local user passwords** that may be compromised.
  - **Updated OpenSSH library** to latest stable version.
- **Simplified Support and Troubleshooting**
  - **Download all logs and diagnostics with a single click** from the **Diagnostics** page for faster support resolution.
  - **Dashboard text field for description enhancement** for reliable appliance identification.

- **Improved Signature Download Security**

  Signature download via proxy now uses **HTTPS (via port 443)**, ensuring secure transmission of update files in proxy environments.

- **Wireless Enhancements for the TZ Wireless series**

  Support for **WAN failover and load balancing** in **wireless station mode** to improve **connection drops or transitions**, helping maintain consistent connectivity.

- **Cloud Secure Edge (CSE) Improvements**

  - Support for **publishing routes outside the RFC1918 range** to **allow connections to any private resource** through the firewall.
  - Support for **more than 100 firewalls** connecting to the same CSE organization.

Resolved Issues

Issue ID	Issue Description
GEN7-52429	The Cloud Secure Edge (CSE) connector fails to automatically recover after an extended internet outage.
GEN7-52611	NAT policy information in the Access Policy log is not displayed in the log message when Flow Report is enabled.
GEN7-52705	When using NetExtender 10.3.2 (which is not officially supported yet for SonicOS), the **DNS Suffix** setting is not propagated to the client.
GEN7-52710	In a High Availability configuration, a race condition could cause external storage to not be mounted correctly on the secondary device logs and cannot be stored in it.
GEN7-52723	SAML references are included in the Tech Support Report (TSR) when running in Policy Mode even though SAML is not supported in Policy Mode.
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.
GEN7-53020	LDAP server configuration is being removed after making changes on the Authentication Partition and Authentication Partition Policies.
GEN7-53118	For SAML configuration and downloading the XML metadata from an Identity Provider and then importing this XML file to 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.
GEN7-53148	Unable to change the **Public IP Address** under the **Anti-Spam** settings.
GEN7-53199	When importing a Network Security Manager (NSM) template, the firewall deletes static DHCP entries.

Issue ID	Issue Description
GEN7-53438	When using authentication with One-Time Password (OTP), a deadlock may occur and cause the device to reboot.
GEN7-53487	Rate-limiting during login (Brute-Force Protection) is not enabled by default.
GEN7-53566	[Vulnerability] Use of Externally-Controlled Format String (PSIRT Advisory: SNWLID-2025-0013)
GEN7-53577	In a High Availability configuration, when a new access policy is added with **Traffic Shaping** using a certain bandwidth object, the audit module fails to find the name of the bandwidth object and the audit log displays the error `n.forEach is not a function` on the secondary firewall.
GEN7-53664	Size fields (such as the Sent and Received fields) **Website Accessed** and **Website Hit** events from the syslog are missing.
GEN7-53872	Guest WiFi users cannot access the internet when **Enable Policy Page without authentication** is enabled under **Guest Services**.
GEN7-54058	For SAML users, the **Members go straight to the management UI on web login** settings do not work.
GEN7-54183	Syslog ID 1079 is missing the syslog parameters required for Analytics reporting.

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.
GEN7-54348	Changing the **OTP Length**, and then changing it back, results in the error: `Please make sure the minimum length is not greater than the maximum length.`
GEN7-54354	*NSv series and NSsp 15700 only:* Users may experience a decrease in performance when configured for Policy Mode.
GEN7-54380	When **New password must contain 8 characters different from the old password** is enabled, changing the password to one that does not match when using NetExtender or Mobile Connect, an error is displayed: `Login failed - Incorrect username/password. 2 more login attempts before lockout.` This will be addressed in a subsequent release.
GEN7-54531	The firewall management interface is not accessible with HTTPS Port 8080 after changing it from 443. **Workaround:** Use a different port other than 8080.
GEN7-54549	*TZ series only:* the primary storage total size is shown as 0.This should be 16 MB.The Available storage is shown correctly.

Issue ID	Issue Description
GEN7-54564	Unable to import LDAP users belonging to a child domains. When clicking on **Import LDAP Users** and then selecting the primary server from the list, the user list does not include users from the child domain, only listing users only from primary domain. **Workaround:** Selecting **Import from all LDAP servers** will display all of the users from all the configured or learned servers.
GEN7-54568	The Mobile Connect client cannot connect to the SSL VPN if the domain name contains special characters.
GEN7-54569	In a High Availability configuration, locked out IP addresses are not being synchronized with the standby firewall.
GEN7-54598	Locked IP addresses gets unlocked automatically when using the Global VPN Client (GVC) client. IPsec VPN reuses connection caches that are not deleted immediately after the login fails.
GEN7-54698	Starting with SonicOS 7.3.0, password complexity enforcement is enabled by default (requiring both alphanumeric and symbolic characters). If the secondary firewall is reset to the factory default settings (e.g., due to RMA), and the primary firewall still uses legacy password settings, synchronization across firewalls configured for High Availability may fail. Recommended Action: • **Option 1 (Recommended):** Update the primary unit's password policy to match SonicOS 7.3 defaults. See KB • **Option 2:** Adjust the secondary unit’s policy to match the primary's existing configuration. Keeping password policies aligned across High Availability firewalls is essential to avoid synchronization issues.
GEN7-54728	A time-based one-time password (TOTP) sent by email is not sent if the local user password is too short.

Additional References

GEN7-50932, GEN7-51198, GEN7-51893, GEN7-51919, GEN7-51973, GEN7-52056, GEN7-52252, GEN7-52333, GEN7-52351, GEN7-52353, GEN7-52375, GEN7-52489, GEN7-52542, GEN7-52686, GEN7-52688, GEN7-52724, GEN7-52831, GEN7-52871, GEN7-52900, GEN7-52950, GEN7-53081, GEN7-53165, GEN7-53171, GEN7-53209, GEN7-53241, GEN7-53272, GEN7-53413, GEN7-53498, GEN7-53508, GEN7-53536, GEN7-53555, GEN7-53557, GEN7-53573, GEN7-53667, GEN7-53681, GEN7-53690, GEN7-53692, GEN7-53719, GEN7-53744, GEN7-53751, GEN7-53913, GEN7-53934, GEN7-54141, GEN7-54145, GEN7-54182, GEN7-54508

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 - July 2025
Software Version - 7.3.0
232-006386-00 Rev A