SonicOS 8

Release Notes

These release notes provide information about the SonicWall SonicOS 8 release.

SonicOS 8.0.x Versions	SonicOS 8.1.x Version	SonicOS 8.2.x Version
Release Description: Version 8.0.4 provides support for the new TZ280P, TZ280W and NSa 6800	**Release Description:** Version 8.1.0 is a feature release built on top of SonicOS 8.0.0, 8.0.1, 8.0.2 and 8.0.3	**Release Description:** Version 8.2.2 is a feature release built on top of SonicOS 8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.1.0, 8.2.0, and 8.2.1
Upgrade path: Anyone buying a TZ280P or TZ280W or NSa 6800 will start with SonicOS 8.0.4. Anyone operating on previous versions of 8.0.x can upgrade to 8.0.4 to take advantage of bug fixes included.	**Upgrade path:** Anyone operating on SonicOS 8.0.0, 8.0.1, 8.0.2 and 8.0.3 should upgrade to SonicOS 8.1.0 to take advantage of the new features. ⚠ **CAUTION: Firewalls running SonicOS 8.1.0 must not be downgraded to SonicOS 8.0.4. Downgrading may result in configuration incompatibilities, loss of features introduced in later releases, and potential system instability.**	**Upgrade path:** Anyone operating on SonicOS 8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.1.0, 8.2.0, and 8.2.1 should upgrade to SonicOS 8.2.2 to take advantage of the new features and fixes. ⚠ **CAUTION: Downgrading from 8.2.2 to any prior firmware version is not supported. Downgrading could result in the deletion of all LDAP users and a complete reset of all MFA settings.** **If a downgrade is required, all LDAP users and MFA configurations must be manually reconfigured afterward. A full configuration backup is strongly recommended before upgrading.**
Version 8.0.4-8014	Version 8.1.0-8017	Version 8.2.2-8015
Version 8.0.3-8011		Version 8.2.1-8010
Version 8.0.2-8011		Version 8.2.0-8009
Version 8.0.1-8017		
Version 8.0.0-8035		
Version 8.0.0-8037		

SonicOS 8.2.x Version

Version 8.2.2-8015

July 2026

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.

Important

- The TZ80:
  - Must be licensed before it can be configured or used.
  - Must always be connected to the Internet. It cannot be used in a closed network environment.
- Beginning with SonicOS 8.0.0, these SonicPoint devices are no longer supported:
  - SonicPoint-N
  - SonicPoint-NDR
  - SonicPoint-Ni/Ne
  - SonicPoint-ACe/ACi/N2
- Support for the WEP and TKIP security protocols has been deprecated.
- Support for the **Radio Role > Mesh Gateway** has been deprecated in the TZ wireless models.
- Settings from Gen 7 firewalls running SonicOS 7.3.x can be imported into Gen 8 firewalls operating on SonicOS 8.2.2 version.
- All features introduced in SonicOS 7.3.3 are available in SonicOS 8.2.2.

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

TZ Series	Firmware Version	NSa Series	Firmware Version	NSv Series	Firmware Version
TZ80	8.2.2-8015	NSa 2800	8.2.2-8015	NSv XS	8.2.2-8015

TZ Series	Firmware Version	NSa Series	Firmware Version	NSv Series	Firmware Version
TZ280	8.2.2-8015	NSa 3800	8.2.2-8015	NSv S	8.2.2-8015
TZ280P	8.2.2-8015	NSa 4800	8.2.2-8015	NSv M	8.2.2-8015
TZ280W	8.2.2-8015	NSa 5800	8.2.2-8015	NSv L	8.2.2-8015
TZ380	8.2.2-8015	NSa 6800	8.2.2-8015		
TZ380W	8.2.2-8015				
TZ480	8.2.2-8015				
TZ580	8.2.2-8015				
TZ680	8.2.2-8015				

Deprecation Notice

Support for customizing guest login pages using external web servers with the CGI mechanism has been deprecated. This functionality will no longer be enhanced, and customers are advised to migrate to the supported API-based guest login customization mechanism.

For migration guidance and additional details, refer to the following Knowledge Base article: Deprecation of CGI-Based Guest Login Page Customization.

What's New

- **Security Services Enabled by Default**

  Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Botnet Filtering, and Geo-IP Filtering are automatically enabled on SonicOS 8 appliances at the point of registration, without requiring post-deployment configuration.

- **Let's Encrypt Integration**

  SonicOS 8.2.2 now supports the ACME v2 protocol for automated issuance, renewal, and installation of SSL/TLS certificates directly from the firewall.

  - Supports HTTP-01 domain validation.
  - Certificates are renewed automatically ahead of expiry.
  - Configurable from both the SonicOS management UI and CLI.

- **Two-Factor Authentication for GVC**

  TOTP-based two-factor authentication is now available for Global VPN Client (GVC) connections.

- **Indicator of Compromise (IoC) – Hash Detection**

  Administrators can import MD5, SHA-1, and SHA-256 hash lists from threat intelligence feeds (up to 500,000 entries). Files matching an imported hash are blocked in transit and logged for audit purposes.

- **Non-Reversible Password Storage**

  Stored credentials now use one-way cryptographic hashing (bcrypt) rather than a reversible format. Existing credentials are automatically migrated during the first login after the upgrade, and configuration exports no longer contain recoverable credentials. This feature is not enabled by default.

- **SD-WAN Site Support Increase**

  The maximum number of supported SD-WAN sites per SonicOS 8 appliance has increased, extending single-hub SD-WAN coverage for larger branch deployments.

- **SonicOS UI/UX Improvements**

  This release includes a consolidated set of usability improvements across rule and policy pages, App Control, VPN monitoring, and logging, aligned with updated NSM 4.3 terminology:

  - Redesigned change-notification banner, repositioned so it no longer blocks key workflow actions.
  - Standardized placement of Add, Edit, Delete, Move, and Clone controls across Access Rules, NAT Rules, Route Rules, DNS Rules, Content Filter Rules, and App Rules.
  - Create Another option added for NAT, Route, DNS, Content Filter, and App Rules.
  - App Control list now sorts by Category Name, then App Name, then Signature ID, with the selected category persisting across changes.
  - VPN tunnel status now updates in real time.
  - ACL/NAT live counters no longer force a full grid reload or lose the last-hit timestamp.
  - Log entries now link directly to the related App Control, IPS, or Anti-Spyware signature settings.
  - LLDP now supports both transmit (Tx) and receive (Rx).
  - The Network > System > Interfaces page supports ascending and descending sort, with sub-interfaces sorted within their parent.

- **SonicOS 8 NSv Small / Medium / Large**

  Three new SonicOS 8 NSv virtual firewall sizes are introduced: Small (2 vCPU / 2 GB), Medium (4 vCPU / 8 GB), and Large (8 vCPU / 16 GB), supporting VMware, KVM, Hyper-V, Proxmox, AWS, and Azure. The maximum supported number of groups per NSv instance has increased to 500.

- **NSM Enhancements**

  SonicOS 8.2.2 is a co-release with NSM 4.3, which includes the following firewall-side capabilities:

  - Source and destination MAC addresses are now captured for user-based system events, including sessions established via SSL VPN or GVC remote access clients.
  - Firewall audit log data can now be delivered to NSM as flow events via a new IPFIX template.

- **User Management Enhancements**

  Guest Wi-Fi now supports a branded captive portal experience with Acceptable Use Policy (AUP) enforcement. RADIUS attribute support has been extended for advanced identity provider and access management integrations.

- **Platform Capacity Increases**
  The following per-platform limits have been increased in this release:
  - TZ80: maximum concurrent SSL VPN users increased to 10.
  - NSv L Model: maximum supported groups increased to 500.

This release also resolves previously reported issues.

Resolved Issues

Issue ID	Description
GEN8-14363	Host header injection vulnerability in SonicOS (CVSS 4.3 - Medium).
GEN8-15431	SD-WAN load balancing does not occur when the SLA strategy is set to Lowest Cost with the LB type set to Ratio.
GEN8-15723	Unable to pass traffic over a LAG member when its LAG Agg is disabled on NSa 2800.
GEN8-16196	NSa 3800 intermittently reports false fan failure alerts.
GEN8-16283	The tooltip on the Geo-IP Filter Settings page was too narrow to display its full text.
GEN8-16355	An error pops up when opening an SSH terminal session in the GUI using the Firefox browser.
GEN8-16421	Bandwidth management parameters under access rules display an incorrect value.
GEN8-16558	Sometimes the auto-download of IoC files still occurs even when file auto-download is disabled.
GEN8-16603	SSL VPN UDP packets are dropped on NSa 2800.
GEN8-16711	The GUI displayed IPv6 traffic under the IPv4 traffic view.
GEN8-16932	SSL VPN users are unable to connect when SYN Flood Protection Mode is set to Always Proxy WAN Client Connections on firmware 8.1.0, 8.2.0, and 8.2.1.
GEN8-17108	The firewall drops Cloud Secure Edge (CSE) egress traffic as “Destination IP unreachable” on NSa 4800.
GEN8-17115	After a factory default, navigating to the Access Rules page and downloading a TSR shows “Licensing must be activated for this feature”.

Known Issues

Issue ID	Description
GEN8-2677	The user is not logged out from the firewall even after the inactivity time is reached.
GEN8-10895	On NSa 6800, a 40G Twinax connection shows no link when the port is set to auto-negotiation; it works only in 40G force mode with Cisco.

Issue ID	Description
GEN8-11359	NSa 4800 intermittently does not detect SFP modules when 10GBASE-T type SFPs are frequently plugged and unplugged.
GEN8-15639	An NSv firewall drops Cloud Secure Edge (CSE) client traffic after a fresh deployment; traffic works only after a firewall reboot.
GEN8-16066	Hashed passwords break the CLDAP periodic check functionality.
GEN8-16864	Admin/user IP lockout does not work for NSv S/M/L on AWS Pay-As-You-Go with UPE/Policy mode; it works on hardware platforms.
GEN8-17572	On NSa 2800, traffic fails after a reboot or restart when the X0 LAG Aggregator is disabled.
GEN8-17959	The “No space available on device” error appears during firmware upload when ZTv3 debug logging is enabled and set to level 13.
GEN8-17990	When storing user passwords non-reversibly is enabled, a new user's password is stored non-reversibly even when the user's group memberships specify that it should be stored reversibly.
GEN8-18136	TACACS user authentication fails when the user logs in with a domain name for the SSL VPN portal.
GEN8-18145	On the System Monitor Real-Time Charts, Interface Usage data is not displayed consistently.
GEN8-18167	Botnet Filtering is automatically enabled after upgrading from 8.2.1 to 8.2.2, even if it was disabled in 8.2.1.
GEN8-18178	On an NSa 6800 HA pair, saving an SSL VPN-to-LAN access rule on a sub-interface with Allow Management Traffic enabled (Optional Settings > Others) returns an error.
GEN8-18187	The Test Email function for SFR mailing returns an “API not found” error.
GEN8-18311	On an NSv firewall, vMotion cannot be enabled from the diagnostics page.
GEN8-18376	A raw API error appears when performing a global search.

Additional References

GEN8-16053, GEN8-16192, GEN8-16222, GEN8-16270, GEN8-16281, GEN8-16357, GEN8-16382, GEN8-16406, GEN8-16424, GEN8-16446, GEN8-16605, GEN8-16608, GEN8-16615, GEN8-16625, GEN8-16650, GEN8-16707, GEN8-16865, GEN8-16916, GEN8-16970, GEN8-16997, GEN8-17149, GEN8-17256, GEN8-17493, GEN8-17546, GEN8-17734

Version 8.2.1-8010

June 2026

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.

Important

- The TZ80:
  - Must be licensed before it can be configured or used.
  - Must always be connected to the Internet. It cannot be used in a closed network environment.
- Beginning with SonicOS 8.0.0, these SonicPoint devices are no longer supported:
  - SonicPoint-N
  - SonicPoint-NDR
  - SonicPoint-Ni/Ne
  - SonicPoint-ACe/ACi/N2
- Support for the WEP and TKIP security protocols has been deprecated.
- Support for the **Radio Role > Mesh Gateway** has been deprecated in the TZ wireless models.
- Settings from Gen 7 firewalls running SonicOS 7.3.x can be imported into Gen 8 firewalls operating on SonicOS 8.2.1 version.

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

TZ Series	Firmware Version	NSa Series	Firmware Version	NSv Series	Firmware Version
TZ80	8.2.1-8010	NSa 2800	8.2.1-8010	NSv XS	8.2.1-8010
TZ280	8.2.1-8010	NSa 3800	8.2.1-8010		
TZ280P	8.2.1-8010	NSa 4800	8.2.1-8010		
TZ280W	8.2.1-8010	NSa 5800	8.2.1-8010		
TZ380	8.2.1-8010	NSa 6800	8.2.1-8010		
TZ380W	8.2.1-8010				

TZ Series	Firmware Version	NSa Series	Firmware Version	NSv Series	Firmware Version
TZ480	8.2.1-8010				
TZ580	8.2.1-8010				
TZ680	8.2.1-8010				

Deprecation Notice

Support for customizing guest login pages using external web servers with the CGI mechanism has been deprecated. This functionality will no longer be enhanced, and customers are advised to migrate to the supported API-based guest login customization mechanism.

For migration guidance and additional details, refer to the following Knowledge Base article: Deprecation of CGI-Based Guest Login Page Customization.

What's New

- **Introduction of a virtual firewall using a single processing core named NSv XS**

  A new single-core NSv model has been introduced for lower-end cloud use cases, providing a lightweight virtual firewall option for resource-constrained environments.

- **Active/Active DPI**

  SonicOS 8.2.1 introduces Active/Active Deep Packet Inspection (DPI) support on NSa 4800, NSa 5800, and NSa 6800 platforms, enabling high-availability deployments with full DPI capabilities across both active units.

- **Enhanced IPv6 Support (Japan JPIX)**

  IPv6 enhancements have been added to support the Japan JPIX "v6plus" Static IP service, meeting regional ISP requirements for Japanese deployments.

- **Syslog Support over TCP and TLS 1.3**

  Syslog transmission can now be secured using TLS 1.3, and syslog processing has been offloaded to the data plane for improved performance and reliability.

- **Indicator of Compromise (IoC) Support — IP Address**

  SonicOS 8.2.1 introduces IP-based IoC detection, enabling the firewall to automatically identify and act on known malicious IP addresses.

- **SDWAN 2.0 Enhancements**

  Multiple SD-WAN 2.0 enhancements are included in this release:

  - Support for ANY Zone (WAN and all non-VPN) and mixing of non-VPN zones in SD-WAN policies
  - Bandwidth usage monitoring in SD-WAN 2.0
  - SLA Strategy selection is now available in SD-WAN path selection
  - Interface Cost configuration added to SD-WAN
  - Cloud-defined SLA Thresholds for popular applications
  - HTTP/HTTPS probe options for SD-WAN path monitoring
  - Schedule per rule support in SD-WAN
  - Load Balancing Mode added in Path Selection Profile.

This maintenance release also resolves previously reported issues.

- SonicOS 8.2.1 supports the TZ80, TZ280, TZ280P, TZ280W TZ380, TZ380W, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800, NSa 6800, and NSv XS.
- SonicOS 8.2.1 includes in-product migration, where you can import settings from your:
  - SonicOS Gen 6/6.5 devices to your new SonicOS Gen 8 devices.
  - SonicWall SOHO/SOHOW security appliance to your new SonicWall TZ80.
  - SonicWall TZ270 security appliance to your new SonicWall TZ280.
  - SonicWall TZ570P security appliance to your new SonicWall TZ280P.
  - SonicWall TZ270W security appliance to your new SonicWall TZ280W.
  - SonicWall TZ370 security appliance to your new SonicWall TZ380.
  - SonicWall TZ370W security appliance to your new SonicWall TZ380W.
  - SonicWall TZ470 security appliance to your new SonicWall TZ480.
  - SonicWall TZ570 security appliance to your new SonicWall TZ580.
  - SonicWall TZ670 security appliance to your new SonicWall TZ680
  - SonicWall NSa 2600 or NSa 2700 security appliance to your new NSa 2800.
  - SonicWall NSa 3600 or NSa 3700 security appliance to your new NSa 3800.
  - SonicWall NSa 4600 or NSa 4700 security appliance to your new NSa 4800.
  - SonicWall NSa 5600 or NSa 5700 security appliance to your new NSa 5800.
  - SonicWall NSa 6600 or NSa 6700 security appliance to your new NSa 6800.

  For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.

  - SonicWall NSv 10, NSv 25, NSv 50, and NSv 100 virtual security appliance to your new NSv XS.

  For more information, refer to the SonicOS 8 Upgrade Guide for the NSv Series.

Resolved Issues

Issue ID	Description
GEN8-8528	**DNS Security** > **DNS Report** > **Host** shows same hostnames for multiple IPs listed on this page.
GEN8-11776	Account lifetime field shows abnormal value after local user account expiration.

Issue ID	Description
GEN8-12871	Unable to delete systemlogs storage file through SonicOS CLI.
GEN8-13422	SAML profile is available for deletion even when it is in use.
GEN8-14510	Clicking **Clear Database** on **Policy** > **DNS Security** > **Reports** displays **API endpoint is incomplete**.
GEN8-14580	Unable to edit the changes for **Restrict access until password changed** in local users section.
GEN8-14852	Default BWM action objects are missing in the App Rules tab.
GEN8-14881	GUI keeps loading when changing **All** to **Default** on **Device** > **Users** > **Partitions** > **Partitions Selection Policies**. No errors displayed in UI either.
GEN8-14883	Partition policy details cannot be displayed correctly when re-editing Partition policy in **Users** > **Partitions** tab.
GEN8-14890	The mail OTP user login always fails when **Enforce login uniqueness** option is enabled.
GEN8-16034	Websites randomly stop working when Client DPI-SSL is enabled on TZ 470, requiring a reboot to restore functionality.

Known Issues

Issue ID	Description
GEN8-15431	SDWAN load balancing is not happening when the SLA strategy is set to Lowest Cost with LB type as Ratio and SDWAN group members are unnumbered VPN tunnel interfaces. **Workaround 1:** If you intend to change the unnumbered interface name and it is part of an SD-WAN load balance config, remove it from the SD-WAN group, rename the unnumbered tunnel interface, then add it back. **Workaround 2:** If the unnumbered interface name change has already occurred, rename the interface back to the name used in the SD-WAN load balance configuration.
GEN8-15624	When using a 40G port as the HA Control Interface on NSa 6800, restarting the standby firewall may intermittently result in **Not receiving heartbeats from peer firewall**, causing it to become Active while the HA peer enters electing mode.
GEN8-15723	Unable to pass traffic over a LAG member when its LAG Agg is disabled on NSa 2800.

Issue ID	Description
GEN8-16032	When Active/Active DPI HA is enabled on the primary firewall and the secondary is in an unregistered (no license) state, the HA mode setting is not synced on the secondary and an error is returned on the HA settings and advanced page. **Workaround 1 (Recommended):** Register both primary and secondary firewalls separately before enabling Active/Active DPI HA. **Workaround 2:** If the issue has already occurred, manually register the secondary firewall; the Active/Active DPI HA setting can then sync successfully.
GEN8-16208	When adding a syslog server entry, no Address Objects appear in the **Name or IP Address** dropdown list. **Workaround:** Create an address object from the syslog server **Name or IP Address** dropdown; after creation, all existing address objects will be listed.
GEN8-16355	An error pops up when opening an SSH terminal session in the GUI using the Firefox browser.
GEN8-16413	SD-WAN path selection profile shows members as not qualified after reboot. The issue occurs with the Lowest Cost strategy in HA mode when all available HA units reboot simultaneously. **Workaround:** Update the cost of the affected interface to a different value, then revert it back to the original value.
GEN8-16551	The SD-WAN Wizard Group settings page is missing Priority, Cost, and Bandwidth configuration options. **Workaround:** After completing the SD-WAN setup guide, go to the **SD-WAN** settings page to manually configure these values.
GEN8-16555	KVM/Proxmox VM management operations (Shutdown/Reboot) time out and fail to execute on NSv XS.
GEN8-16558	Sometimes the auto-download of IoC files still occurs even when file auto-download is disabled.

Additional References

GEN8-16409, GEN8-16112, GEN8-15848, GEN8-15846, GEN8-15666, GEN8-15579, GEN8-15536, GEN8-15237, GEN8-15227, GEN8-14783, GEN8-14443, GEN8-14133, GEN8-14119, GEN8-13882, GEN8-13878, GEN8-13840, GEN8-13822, GEN8-12671

Version 8.2.0-8009

February 2026

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.

Important

- The TZ80:
  - Must be licensed before it can be configured or used.
  - Must always be connected to the Internet. It cannot be used in a closed network environment.
- Beginning with SonicOS 8.0.0, these SonicPoint devices are no longer supported:
  - SonicPoint-N
  - SonicPoint-NDR
  - SonicPoint-Ni/Ne
  - SonicPoint-ACe/ACi/N2
- Support for the WEP and TKIP security protocols has been deprecated.
- Support for the **Radio Role > Mesh Gateway** has been deprecated in the TZ wireless models.
- Settings from Gen 7 firewalls running SonicOS 7.3.x can be imported into Gen 8 firewalls operating on SonicOS 8.2.0 version.

NetExtender Compatibility & Bundling Update

- **New Version Support**: SonicOS 8.2.0 introduces official support for **NetExtender version 10.3.4**, while maintaining backward compatibility with the **NetExtender version 10.2.x** branch.
- **Upgrade Recommendation**: To ensure the highest level of security and performance, it is strongly recommended that customers upgrade all NetExtender clients to **version 10.3.4** at their earliest convenience.

- **Transition & Integration Details**:
  - **Bundled Version**: SonicOS 8.2.0 is now natively bundled with **NetExtender version 10.3.4**.
  - **Transition Benefit**: This ensures that new deployments and upgrades automatically provide users with the latest recommended client version.

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

TZ Series	Firmware Version	NSa Series	Firmware Version
TZ80	8.2.0-8009	NSa 2800	8.2.0-8009
TZ280	8.2.0-8009	NSa 3800	8.2.0-8009
TZ280P	8.2.0-8009	NSa 4800	8.2.0-8009
TZ280W	8.2.0-8009	NSa 5800	8.2.0-8009
TZ380	8.2.0-8009	NSa 6800	8.2.0-8009
TZ380W	8.2.0-8009		
TZ480	8.2.0-8009		
TZ580	8.2.0-8009		
TZ680	8.2.0-8009		

Deprecation Notice

Support for customizing guest login pages using external web servers with the CGI mechanism has been deprecated. This functionality will no longer be enhanced, and customers are advised to migrate to the supported API-based guest login customization mechanism.

For migration guidance and additional details, refer to the following Knowledge Base article: Deprecation of CGI-Based Guest Login Page Customization.

What's New

- **Credential Auditor**
  SonicOS 8.2.0 supports Credential Auditor, a built-in security feature designed to strengthen password protection. It automatically checks user credentials against known lists of compromised passwords, flags any matches, and enables administrators to take immediate action such as issuing warnings or enforcing password changes. This capability is included at no additional cost, with no extra SKUs or products required. Credential Auditor provides customers and partners with a simple, proactive way to manage credential risks, further enhancing SonicWall's integrated, easy-to-use.
- **Enhanced Security Default**
  Updated OpenSSH library to the 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 downloads via proxy now use **HTTPS (port 443)**, ensuring the secure transmission of update files in proxy environments.
- **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.
- Support for Bearer Token Validation for Non-GUI API Sessions

  The **Two-Factor and Bearer Token Authentication** option has been renamed to **Non-GUI Management Login Bearer Token Session Check**.

  This security option introduces **bearer token validation for non-GUI (API-only) sessions**, enhancing authentication control for API access.

  Key Details:
  - This option is **turned off by default**, including after a factory reset.
  - When enabled, the firewall issues a **bearer token** in the **/auth** API response.
  - All subsequent non-GUI API requests must include this bearer token in the request header for authentication.

  For more information and configuration details, refer to the following Knowledge Base article: Support for Bearer Token Validation for Non GUI API Sessions.

This maintenance release also resolves previously reported issues.

- SonicOS 8.2.0 supports the TZ80, TZ280, TZ280P, TZ280W TZ380, TZ380W, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, NSa 5800, and NSa 6800.

- SonicOS 8.2.0 includes in-product migration, where you can import settings from your:
  - SonicOS Gen 6/6.5 devices to your new SonicOS Gen 8 devices.
  - SonicWall SOHO/SOHOW security appliance to your new SonicWall TZ80.
  - SonicWall TZ270 security appliance to your new SonicWall TZ280.
  - SonicWall TZ570P security appliance to your new SonicWall TZ280P.
  - SonicWall TZ270W security appliance to your new SonicWall TZ280W.
  - SonicWall TZ370 security appliance to your new SonicWall TZ380.
  - SonicWall TZ370W security appliance to your new SonicWall TZ380W.
  - SonicWall TZ470 security appliance to your new SonicWall TZ480.
  - SonicWall TZ570 security appliance to your new SonicWall TZ580.
  - SonicWall TZ670 security appliance to your new SonicWall TZ680
  - SonicWall NSa 2600 or NSa 2700 security appliance to your new NSa 2800.
  - SonicWall NSa 3600 or NSa 3700 security appliance to your new NSa 3800.
  - SonicWall NSa 4600 or NSa 4700 security appliance to your new NSa 4800.
  - SonicWall NSa 5600 or NSa 5700 security appliance to your new NSa 5800.
  - SonicWall NSa 6600 or NSa 6700 security appliance to your new NSa 6800.

  For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.

Resolved Issues

Issue ID	Description
GEN8-6895	Post-authentication Stack-based Buffer Overflow vulnerability (SNWLID-2026-0004).
GEN8-12981	Improper Access Control Vulnerability (SNWLID-2026-0004).
GEN8-13158	Post-Authentication Path Traversal Vulnerability (SNWLID-2026-0004).
GEN8-13779	Unexpected audit log **Interface LAN/DMZ L2 Bridged Mode: VLAN Filtering Mode** reported when editing interfaces.
GEN8-14136	Port redundancy could be configured on incompatible interfaces on NSA 2800 and was removed after reboot.
GEN8-14145	High Availability could not be established due to **admin sync fail**.
GEN8-14180	Log priority changed when creating a configuration file for NSA3800 from NSA3600 using the Migration App on NSM.
GEN8-14218	TOTP not working for NetExtender when using LDAP users.
GEN8-14427	Post-authentication stack-based buffer overflow (SNWLID-2026-0001).
GEN8-14444	Default HTTPS management NAT rule on NSA 2700 returns to top priority after reboot and firmware upgrade.
GEN8-14898	Certain configuration of SSO Terminal Service Agent causes TZ670 device to reboot after upgrade.

Known Issues

Issue ID	Description
GEN8-13375	Virus, Spyware, and IPS cannot be detected when downloading via DPI-SSH from a Windows client.
GEN8-14436	Packets from Layer2 LAG Interface to WAN are dropped and not forwarded.
GEN8-14510	Clicking **clear database** on **Policy** → **DNS Security** → **Reports** displays **API endpoint is incomplete**.
GEN8-14580	Restrict access until password change is not editable for local users.
GEN8-14795	X6 OSPF cannot be set to Passive mode or changed back to Disabled.
GEN8-14852	BWM action objects are missing for HTTP Client policy type in App rules.
GEN8-14881	GUI keeps loading when changing **All** to **Default** on **Device** → **Users** → **Partitions** → **Partitions Selection Policies**.

Additional References

Not Applicable.

SonicOS 8.1.x Version

Version 8.1.0-8017

November 2025

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.

Important

- The TZ80:
  - Must be licensed before it can be configured or used.
  - Must always be connected to the Internet. It cannot be used in a closed network environment.
- Beginning with SonicOS 8.0.0, these SonicPoint devices are no longer supported:
  - SonicPoint-N
  - SonicPoint-NDR
  - SonicPoint-Ni/Ne
  - SonicPoint-ACe/ACi/N2
- Support for the WEP and TKIP security protocols has been deprecated.
- Support for the **Radio Role > Mesh Gateway** has been deprecated in the TZ wireless models.
- Settings from Gen 7 firewalls running SonicOS 7.3.x cannot be imported into Gen 8 firewalls operating on SonicOS 8.1.0 due to version incompatibility. However, SonicOS 8.2.0, planned for all Gen 8 firewalls, will introduce support for importing configurations from SonicOS 7.3.x, enabling a streamlined migration process.

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

TZ Series	Firmware Version	NSa Series	Firmware Version
TZ80	8.1.0-8017	NSa 2800	8.1.0-8017
TZ280	8.1.0-8017	NSa 3800	8.1.0-8017
TZ380	8.1.0-8017	NSa 4800	8.1.0-8017
TZ380W	8.1.0-8017	NSa 5800	8.1.0-8017
TZ480	8.1.0-8017		
TZ580	8.1.0-8017		
TZ680	8.1.0-8017		

What's New

This maintenance release provides the following enhancements and the fixes for previously reported issues.

- **SAML 2.0 support for Generation 8 firewalls**
  SonicOS 8.1.0 provides for SAML-based authentication. See the SonicOS 8 SAML Feature Guide for more information.
- **SonicWall firewalls can act as an NTP server**
  SonicWall Generation 8 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 DPI-SSL CA certificate**

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

- Renewal of DHCP IP addresses on the wireless interface (W0) when the connection drops and returns or when switching networks.
- Support for **Override Default MAC address** on the wireless interface (W0).
- SonicOS 8.1.0 supports the TZ80, TZ280, TZ380, TZ380W, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, and NSa 5800.
- SonicOS 8.1.0 includes in-product migration where you can import settings from your:
  - SonicOS Gen 6/6.5 devices to your new SonicOS Gen 8 devices.
  - SonicOS Gen 7 devices to your new SonicOS Gen 8 devices.

  For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.

Resolved Issues

Issue ID	Issue Description
GEN8-12269	NetExtender 10.3.2 - Unable to authenticate to Duo Proxy MFA (issue not present in NetExtender 10.2).
GEN8-12082	An error when creating a user group with @ in the name via SNMP through the GUI.
GEN8-11711	With a wireless client connected to the Access Point, the monitor page always shows the allow and deny buttons in grey, even if the ACL function is enabled or disabled.
GEN8-11640	Setting the schedule for Firmware Auto Update causes an error when using Safari to access the UI.
GEN8-11638	App Rule number of times matched shows Zero when the app rule policy name is followed by a space.
GEN8-11523	No error is returned when selecting a certificate without Server Authentication enabled for SSLVPN service.
GEN8-11467	NSv series and NSsp 15700 only: Users may experience a decrease in performance when configured for Policy Mode.
GEN8-11155	The **User Domain** field does not appear after switching the SSLVPN **Authentication Type** to certificate.
GEN8-9886	Cannot use custom SSL VPN zone object in SSL VPN client profile configuration.

Issue ID	Issue Description
GEN8-8749	Failed to search for an LDAP user with Qualified Login Name due to error '**qualified-name** is not a valid value'.

Known Issues

Issue ID	Issue Description
GEN8-14075	Diag page in SonicOS 8.1.0 doesn’t display option for scp host key check.
GEN8-13422	The SAML profile in use for SSL VPN or management should not be deleted.
GEN8-13411	NSa3800 -HA -- The primary firewall crashed due to tLdapAsyncTask (0x7f4204ef2640) during mixed traffic execution.
GEN8-13152	DPI SSH didn't work on NSv Policy & Global mode.
GEN8-12954	Primary active TZ680 is stuck in **SYNC** status, and HA sync is lost after importing a batch of LDAP users (50+) local.
GEN8-12949	Logging out an SSO user will also log out the SAML user on the same IP.
GEN8-12912	When switching the storage device in the CLI, the GUI displays correctly, but the stored file remains on the previous storage device.
GEN8-12871	Cannot delete the system logs storage file using the CLI, even though the CLI output indicates **change made**.
GEN8-12822	Firewall is rebooting when changing the Local user's Domain from Any to a custom LDAP Domain.
GEN8-12706	Licensing Enforce Grace Period and Enforce Packet Blocking do not take effect without a reboot.
GEN8-12561	Active 2800 crashed at tSyncComTask when running HTTPS traffic over TI VPN tunnels with 3k clearpass sessions logged on.
GEN8-12114	Support Mouse Inactivity Check on NetExtender 10.3.x.
GEN8-11956	Wireless drive issue that causes FW hang and gets rebooted after 1-2 hours of wireless stability testing.
GEN8-11939	The local user has an Unlimited remaining session time.
GEN8-11882	LDAP users cannot change expired passwords using RADIUS MS-CHAPv2 as a fallback when LDAP is set for authentication.
GEN8-11779	An expired user can still log in through the SSL VPN portal when using certificate authentication.
GEN8-11776	The account lifetime field shows an abnormal value after the user account expiration.
GEN8-11361	tCLIPipe-S0 core dump observed when accessing Monitor / Logs / System Logs on the secondary ACTIVE node.

Additional References

Not Applicable.

SonicOS 8.0.x Versions

Version 8.0.4-8014

December 2025

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.

Important

- The TZ80:
  - Must be licensed before it can be configured or used.
  - Must always be connected to the Internet. It cannot be used in a closed network environment.
- Beginning with SonicOS 8.0.0, these SonicPoint devices are no longer supported:
  - SonicPoint-N
  - SonicPoint-NDR
  - SonicPoint-Ni/Ne
  - SonicPoint-ACe/ACi/N2
- Support for the WEP and TKIP security protocols has been deprecated.
- Support for the **Radio Role > Mesh Gateway** has been deprecated in the TZ wireless models.
- Settings from Gen 7 firewalls running SonicOS 7.3.x cannot be imported into Gen 8 firewalls operating on SonicOS 8.0.4 or 8.1.0 due to version incompatibility. However, SonicOS 8.2.0, planned for all Gen 8 firewalls, will introduce support for importing configurations from SonicOS 7.3.x, enabling a streamlined migration process.

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

TZ Series	Firmware Version	NSa Series	Firmware Version
TZ80	8.0.4-8014	NSa 2800	8.0.4-8014
TZ280	8.0.4-8014	NSa 3800	8.0.4-8014
TZ280P	8.0.4-8014	NSa 4800	8.0.4-8014
TZ280W	8.0.4-8014	NSa 5800	8.0.4-8014
TZ380	8.0.4-8014	NSa 6800	8.0.4-8014
TZ380W	8.0.4-8014		
TZ480	8.0.4-8014		
TZ580	8.0.4-8014		
TZ680	8.0.4-8014		

What's New

This maintenance release introduces additional support and resolves previously reported issues.

- SonicOS 8.0.4 adds support for the TZ280P, TZ280W and NSa 6800.
- SonicOS 8.0.4 supports the TZ80, TZ280, TZ380, TZ380W, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800, and NSa 5800.
- SonicOS 8.0.4 includes in-product migration, where you can import settings from your:
    - SonicOS Gen 6/6.5 devices to your new SonicOS Gen 8 devices.
    - SonicWall SOHO/SOHOW security appliance to your new SonicWall TZ80.
    - SonicWall TZ270 security appliance to your new SonicWall TZ280.
    - SonicWall TZ570P security appliance to your new SonicWall TZ280P.
    - SonicWall TZ270W security appliance to your new SonicWall TZ280W.
    - SonicWall TZ370 security appliance to your new SonicWall TZ380.
    - SonicWall TZ370W security appliance to your new SonicWall TZ380W.
    - SonicWall TZ470 security appliance to your new SonicWall TZ480.
    - SonicWall TZ570 security appliance to your new SonicWall TZ580.
    - SonicWall TZ670 security appliance to your new SonicWall TZ680
    - SonicWall NSa 2600 or NSa 2700 security appliance to your new NSa 2800.
    - SonicWall NSa 3600 or NSa 3700 security appliance to your new NSa 3800.
    - SonicWall NSa 4600 or NSa 4700 security appliance to your new NSa 4800.
    - SonicWall NSa 5600 or NSa 5700 security appliance to your new NSa 5800.
    - SonicWall NSa 6600 or NSa 6700 security appliance to your new NSa 6800.

  For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.

Resolved Issues

Issue ID	Issue Description
GEN8-12036	UI returns an error when trying to create an SNMP user group with an '@' in the name.
GEN8-12007	Failed to authenticate to Duo Proxy MFA with NetExtender 10.3.
GEN8-11345	User sessions on the **Device > Users > Status** page will disappear when using NetExtender to connect with an IPv6 address.
GEN8-11185	IPv6 VLAN interface sends RA packets with the wrong source MAC address.
GEN8-11159	Getting error **API endpoint is incomplete** when trying to delete all packet capture files from the secondary storage files page.
GEN8-10897	Locked out IP addresses are not syncing with the HA standby node.
GEN8-10884	M1 storage card lacks any card info (Serial, SN, storage sig, etc.) in the system log.
GEN8-10870	Inactivity timeout is not functioning for SSLVPN web portal connections.
GEN8-10839	VLAN sub-interface subnet route policies are greyed out after firmware upgrade on HA setup.
GEN8-10805	The security LED on the front panel turns from green to off after uploading a firmware.
GEN8-10740	Console prints **i801_smbus 0000:00:1f.4: SMBus is busy, can't use it!** When NSa4800/5800 powers on with a 1G SFP module, Finisar FCMJ-8520-3 is plugged in.
GEN8-10323	Sometimes traffic fails after HA failover when HA Virtual MAC and Override Virtual MAC are enabled simultaneously.
GEN8-5960	UI error **Request failed with status code 400** occurs when importing over 100 LDAP users.
GEN8-5635	The mail OTP user login always fails when the **Enforce login uniqueness** option is enabled.

Known Issues

Issue ID	Issue Description
GEN8-13779	Unexpected audit log **Interface LAN/DMZ L2 Bridged Mode: VLAN Filtering Mode** reported when editing interfaces.
GEN8-10813	**Override Default MAC Address** on W0 Interface is not supported.
GEN8-10812	Raised the DNS proxy rule limit to 1024.

Issue ID	Issue Description
GEN8-7283	WPA2/WPA3-EAP is not supported on TZs with an internal wireless module operating in station mode.
GEN8-5439	User Status INACTIVITY REMAINING shows "**No Data**" for user login through IPv6.

Additional References

GEN8-13556, GEN8-13494, GEN8-13333, GEN8-13332, GEN8-13104, GEN8-12761, GEN8-12673, GEN8-11305, GEN8-11143, GEN8-10837.

Version 8.0.3-8011

August 2025

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

TZ Series	Firmware Version	NSa Series	Firmware Version
TZ80	8.0.3-8011	NSa 2800	8.0.3-8011
TZ280	8.0.3-8011	NSa 3800	8.0.3-8011
TZ380	8.0.3-8011	NSa 4800	8.0.3-8011
TZ380W	8.0.3-8011	NSa 5800	8.0.3-8011
TZ480	8.0.3-8011		
TZ580	8.0.3-8011		
TZ680	8.0.3-8011		

ⓘ | **IMPORTANT:**

- The TZ80:
  - Must be licensed before it can be configured or used.
  - Must always be connected to the Internet. It cannot be used in a closed network environment.

- Beginning with SonicOS 8.0.0, these SonicPoint devices will no longer be supported:
    - SonicPoint-N
    - SonicPoint-NDR
    - SonicPoint-Ni/Ne
    - SonicPoint-ACe/ACi/N2
- Support for the WEP and TKIP security protocols has been deprecated.
- Support for the Radio Role > Mesh Gateway has been deprecated in the TZ wireless models.

What's New

- SonicOS 8.0.3 adds support for the TZ280, TZ380W, TZ580, NSa 4800, and NSa 5800.
- SonicOS 8.0.3 includes in-product migration where you can import settings from your:
    - SonicWall SOHO/SOHOW security appliance to your new SonicWall TZ80.
    - SonicWall TZ270 security appliance to your new SonicWall TZ280.
    - SonicWall TZ370 security appliance to your new SonicWall TZ380.
    - SonicWall TZ370W security appliance to your new SonicWall TZ380W.
    - SonicWall TZ470 security appliance to your new SonicWall TZ480.
    - SonicWall TZ570 security appliance to your new SonicWall TZ580.
    - SonicWall TZ 670 security appliance to your new SonicWall TZ680
    - SonicWall NSa 2600 or NSa 2700 security appliance to your new NSa 2800.
    - SonicWall NSa 3600 or NSa 3700 security appliance to your new NSa 3800.
    - SonicWall NSa 4600 or NSa 4700 security appliance to your new NSa 4800.
    - SonicWall NSa 5600 or NSa 5700 security appliance to your new NSa 5800.

  For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.

This maintenance release provides fixes for previously reported issues

Resolved Issues

Issue ID	Issue Description
GEN8-11038	Guest Wi-Fi users cannot access the internet with the **Enable Policy Page without authentication** option enabled under Guest Services.
GEN8-10726	When the password is changed, but doesn't meet the security requirement for 8 different characters from the old password, the warning message is not properly displayed.
GEN8-10638	The Control Plane Flood Protect feature is not enforced and of no use. This was a carryover from previous generations and now being removed from the user interface.
GEN8-10453	When the firmware auto update feature is enabled on an HA deployment, if the new firmware auto download on HA active firewall is slow and takes over 45 seconds to complete, the downloaded firmware cannot be synced to HA idle firewal; hence, the auto install cannot complete as expected. This works as expected on standalone units.

Issue ID	Issue Description
GEN8-10311	Before registration, if you enable the **Enable Logging to Storage** option, then you will be unable to view the logs in the **Monitor > Logs > System Log** page due to the error message **Work around:** Register the firewall.
GEN8-9970	The egress rate for the X1 interface is not shown on the **Monitor > Real-Time Charts > System Monitor** Interface Usage page.
GEN8-9856	Unable to add a FQDN Address object to the Address group which is part of a NAT policy.
GEN8-9855	The certificate error, “HTTPS handshake SSLv3 alert: certificate unknown,”:is seen when accessing the HTTPS Management page.
GEN8-9816	The CSE Connector won't show up until you click the **Synchronize** button on the Device License Registration page.
GEN8-9784	The numbered VPN tunnel interface shows incorrectly when getting the interface (ifOperStatus) using SNMP.

Known Issues

Issue ID	Issue Description
GEN8-11677	NetExtender failed to connect to IPv6 SSLVPN server in the first login when the local user enabled the option **User must change password** in User Settings, after successfully changing the password the next login.
GEN8-11345	The User sessions in **Device> Users > Status** page disappears when using NetExtender to establish connection with IPv6 address.
GEN8-11159	Getting the error **API endpoint is incomplete** when trying to delete all packet capture files from Secondary Storage Files page.
GEN8-11155	**User Domain** field is not displayed after changing SS LVPN **Authentication Type** to **Certificate**.
GEN8-10884	M1 storage card does not have any card information (serial number, etc.) in the system log.
GEN8-10805	The security LED on front panel is changing from Green to off after uploading firmware.
GEN8-10740	Console displays **i801_smbus 0000:00:1f.4: SMBus is busy, can't use it!** when NSa4800 or NSa 5800 firewall powers on with 1G SFP module Finisar FCMJ-8520-3 plugged in.
GEN8-9886	Unable to use custom SSL VPN zone object in SSL VPN client profile configuration.

Additional References

GEN8-10553, GEN8-10910

Version 8.0.2-8011

August 2025

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

Platform	Firmware Version
TZ80	8.0.2-8011
TZ380	8.0.2-8011
TZ480	8.0.2-8011
TZ680	8.0.2-8011
NSa 2800	8.0.2-8011
NSa 3800	8.0.2-8011

ⓘ | **IMPORTANT:**

- The TZ80 must be licensed before it can be configured or used.
- The TZ80 must always be connected to the Internet. It cannot be used in a closed network environment.

Beginning with SonicOS 8.0.0, these SonicPoint devices will no longer be supported:

- SonicPoint-N
- SonicPoint-NDR
- SonicPoint-Ni/Ne
- SonicPoint-ACe/ACi/N2

What's New

- SonicOS 8.0.2 adds support for the NSa 3800.
- SonicOS 8.0.2 adds support for the TZ380, TZ480, and TZ680.

- SonicOS 8.0.2 includes in-product migration where you can import settings from your:
  - SonicWall SOHO/SOHOW security appliance to your new SonicWall TZ80.
  - SonicWall NSa 2600 or NSa 2700 security appliance to your new NSa 2800.
  - SonicWall NSa 3600 or NSa 3700 security appliance to your new NSa 3800.

  For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.

This maintenance release provides fixes for previously reported issues

Resolved Issues

Issue ID	Issue Description
GEN8-6768	The Cloud Secure Edge (CSE) connector fails to automatically recover after an extended internet outage.
GEN8-8050	When connecting to the 10G SFP+ port using a copper twinaxial cable, and disabling the 10G port in the management interface, the link is still active in the peer device.
GEN8-8721	The console displays the error message `snwl_mv_cpss_lacp_port_tcam_flood_block: src port 15 dst port 10 cpssDxChVirtualTcamRuleWrite FAILED` when adding a link aggregation group on the **Switching > Link Aggregation** page.
GEN8-8798	*NSa 2800 only:* A NSa 2800 firewall cannot be detected by the SonicExpress Setup Guide when using an iPhone connected to the firewall using an USB cable.
GEN8-9022	The console displays the error message `initTcamMgr: cpssDxChVirtualTcamCreate tcam id 3 FAILED rc = [4]` during firewall boot up
GEN8-9768	Unable to add a FQDN Address object to an Address group that is part of a NAT policy.
GEN8-9794	Local users members of SonicWall Administrators group are logged out after 2 minutes while actively working in the management interface when **Open user's login status window in the same window rather than in a popup** is enabled.
GEN8-9814	The error **Account Already in Use** is displayed when a NetExtender user tries to connect to SSL VPN when the SSL VPN session was not removed when two-factor authentication (TFA) failed.
GEN8-9825	A new SonicWall firewall DPI-SSL CA certificate has been added and will require to be distributed if in-use.
GEN8-9831	A **Remote Reset** error is displayed when performing a firewall firmware upgrade using Network Security Manager (NSM) for firewalls with High Availability Stateful Synchronization enabled.
GEN8-9857	Syslog data sent from the firewall is incomplete when SSO is enabled and the zone is configured to be a trusted zone.

Issue ID	Issue Description
GEN8-9866	A failure message is displayed when the reset counters are clicked in the routing rules.
GEN8-9877	Upgrading the firmware to SonicOS 8.0.2 on firewalls configured for in High Availability and managed by NSM: The fix included in the latest SonicOS 8.0.2 release allows upgrading the firmware on firewalls configured for High Availability from SonicOS 8.2.2 to a higher firmware version. To upgrade the firmware to 8.0.2: 1. Disable **High Availability Stateful Synchronization** on the High Availability Active firewall. 2. Restart both of the firewalls configured for High Availability. 3. After the firewalls come up, check and ensure **High Availability Stateful Synchronization** is disabled on both firewalls. 4. Perform the firmware upgrade. 5. After both the High Availability firewalls are upgraded to SonicOS 8.2.2, enable **High Availability Stateful Synchronization**. After the firewalls are upgraded to SonicOS 8.2.2, the next firmware upgrade to a higher version of SonicOS can be performed directly using NSM without having to perform these steps.

Known Issues

Issue ID	Issue Description
GEN8-8692	*NSa 3800 only:* Flow control does not work well on the NSa 3800 when link speed of the port is configured as **Forced** (for example: 1G Full Duplex or 100M Full Duplex).
GEN8-9970	The X1 egress rate is not displayed on the **MONITOR > Real-Time Charts > System Monitor > Interface Usage** page.
GEN8-10311	Before registering the firewall, if **Enable Logging to Secondary Storage** is selected, then the logs that should be visible on **Monitor > Logs > System Log** are not displayed and an error message is displayed instead. **Workaround:** Register the firewall on the **License** page.
GEN8-10323	Sometimes traffic fails after High Availability failover when the High Availability Virtual MAC and Override Virtual MAC are both enabled.

Issue ID	Issue Description
GEN8-10453	When the firmware auto update feature is enabled on firewalls configured for High Availability, if the new firmware auto download on the High Availability active firewall is slow and takes more than 45 seconds to complete, the downloaded firmware cannot be synced to the High Availability idle firewall, and the auto install will not complete as expected. **Workaround:** If your firewall is configured for High Availability, the active firewall auto-downloaded a new firmware, and the firmware does not synchronize to the standby firewall: 1. Delete the uploaded firmware on the active firewall which has been auto-downloaded. 2. On active firewall: a. Manually upload the new firmware. It will be synced to the standby firewall. b. Upgrade the firmware using the manually uploaded firmware. The standby firewall will restart first, then the active firewall will restart with the new firmware.

Additional References

GEN8-10036

Version 8.0.1-8017

May 2025

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

Platform	Firmware Version
TZ80	8.0.1-8017
NSa 2800	8.0.1-8017

ⓘ | **IMPORTANT:** The TZ80 must be licensed before it can be configured or used.

IMPORTANT: The TZ80 must always be connected to the Internet. It cannot be used in a closed network environment.

Beginning with SonicOS 8.0.0, these SonicPoint devices will no longer be supported:

- SonicPoint-N
- SonicPoint-NDR
- SonicPoint-Ni/Ne
- SonicPoint-ACe/ACi/N2

What's New

- SonicOS 8.0.1 adds support for the NSa 2800.
- SonicOS 8.0.1 includes in-product migration where you can import settings from your:
  - SonicWall SOHO/SOHOW security appliance to your new SonicWall TZ80.
  - SonicWall NSa 2600 or NSa 2700 security appliance to your new NSa 2800.

  For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.
- Beginning with SonicOS 8.0.0, support for the security protocols WEP and TKIP has been deprecated.

This maintenance release provides fixes for previously reported issues

Resolved Issues

Issue ID	Issue Description
GEN8-1740	*TZ80 only:* When the X4 port is connected to a Dell Force10 switch or another SonicWall firewall in Auto Negotiate mode, the remote port is negotiated as 1G Half Duplex.
GEN8-5152	TLS displayed as **Disabled** when a LDAP server is automatically added, and displays an error if you try to manually enable TLS.
GEN8-6497	The Setup Wizard displays **Failure: "failed to finish auto-configuration"** on the summary page. After clicking OK, it will proceed, and the Setup Wizard settings are saved and take effect.
GEN8-6581	*TZ80 only:* The license expiration time is inconsistent with MySonicWall due to the time zone difference (+/- 12 hours).
GEN8-6748	When adding a network object `0.0.0.0/8`, the firewall does not display the correct net mask when saved.
GEN8-6761	User login authentication redirection starting from HTTPS URLs is not working in Chrome and Microsoft Edge browser versions 129.0.*x.x* and 130.0.*x.x*.
GEN8-6817	A newly added local user may not be seen until a refresh is done.

Issue ID	Issue Description
GEN8-6833	*TZ80 only:* The Wireless Clients **Configure** button is always grayed out on the **Access Point Monitor**.
GEN8-6864	*TZ80 only:* After the TZ80 starts up, the following error is displayed: **License Manager Unavailable. The firewall can no longer communicate with the Licensing Server (LM/License Manager). Please restore**.
GEN8-7799	SonicWall SSL VPN Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
GEN8-7800	SonicWall SSL VPN Authentication Bypass Vulnerability
GEN8-7801	SonicWall SSH Management Server-Side Request Forgery Vulnerability
GEN8-7824	When a large number of VPN security associations are present in a Stateful High Availability environment, some IKE security associations may not be cleaned up on the secondary device if the synchronization fails.

Known Issues

Issue ID	Issue Description
GEN8-6938	After Cloud Edge Security (Cloud Edge Security) Tunnels are down, it takes a longer time (about 8 minutes) to get the WireGuard Session Disconnect Log even after Cloud Edge Security status shows "down" status.
GEN8-7902	*NSa 2800 only:* Flow control may not function as expected when the link speed of a port is configured as Forced (e.g., 1G Full Duplex,100M Full Duplex).
GEN8-8036	*NSa 2800 only:* The auto-update feature is not automatically installing the downloaded firmware on firewalls in a High Availability configuration when one of firewalls is offline.
GEN8-8050	When the 10G SFP+ port is connected with copper twinax cable, after disabling the 10G port using firewall web management interface, the actual link is still available in the peer device.
GEN8-8125	Logging out multiple selected guest users may not function as expected.
GEN8-8154	The expired IPsec Signature Authority of IKEv2 VPN is not deleted on an idle firewall in a High Availability configuration.
GEN8-8216	*NSa 2800 only:* When importing settings from SonicWall GEN 7 appliances, if there is a L3 LAG or port redundancy created between interfaces that translate to SFP vs. non-SFP, then that L3 LAG or port redundancy will not be created. The settings in general will be imported without any issues. There will be a WARNING displayed in the console logs regarding not creating the L3 LAG and port redundancy.
GEN8-8528	The **DNS Security > DNS Report > Host** page displays the same host names for multiple IP addresses listed on this page.

Issue ID	Issue Description
GEN8-8721	The console displays the error message `snwl_mv_cpss_lacp_port_tcam_flood_block: src port 15 dst port 10 cpssDxChVirtualTcamRuleWrite FAILED` when adding a link aggregation group on the **Switching > Link Aggregation** page.
GEN8-8749	The search fails when searching for a LDAP user with a Qualified Login Name with the error `"qualified-name" is not a reasonable value.`
GEN8-8798	*NSa 2800 only:* A firewall cannot be detected by the SonicExpress Setup Guide when using an iPhone with an USB connection to the firewall.
GEN8-9022	The console displays `cpss failure "initTcamMgr: cpssDxChVirtualTcamCreate tcam id 3 FAILED rc = [4]` while the firewall starts up.

Version 8.0.0-8037

January 2025

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

Platform	Firmware Version
TZ80	8.0.0-8037

IMPORTANT: The TZ80 must be licensed before it can be configured or used.

IMPORTANT: The TZ80 must always be connected to the Internet. It cannot be used in a closed network environment.

Beginning with SonicOS 8.0.0, these SonicPoint devices will no longer be supported:

- SonicPoint-N
- SonicPoint-NDR
- SonicPoint-Ni/Ne
- SonicPoint-ACe/ACi/N2

What's New

- The SonicWall TZ80 offers in-product migration where you can import settings from your SonicWall SOHO/SOHOW security appliance to your new SonicWall TZ80. For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.
- Beginning with SonicOS 8.0.0, support for the security protocols WEP and TKIP has been deprecated.

Resolved Issues

Issue ID	Issue Description
GEN8-7794	SonicOS SSL VPN Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (SNWLID-2025-0003)
GEN8-7795	SonicOS SSL VPN Authentication Bypass Vulnerability (SNWLID-2025-0003)
GEN8-7796	SonicOSSSH Management Server-Side Request Forgery Vulnerability (SNWLID-2025-0003)
GEN8-7874	SSL-VPN MFA Bypass Due to UPN and SAM Account Handling in Microsoft Active Directory (SNWLID-2025-0001)
GEN8-7875	SonicOS Post-authentication arbitrary file read vulnerability (SNWLID-2025-0004)
GEN8-7876	SonicOS Post-authentication format string vulnerability (SNWLID-2025-0004)

Additional References

GEN8-7793

Version 8.0.0-8035

November 2024

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

Platform	Firmware Version
TZ80	8.0.0-8035

IMPORTANT: The TZ80 must be licensed before it can be configured or used.

IMPORTANT: The TZ80 must always be connected to the Internet. It cannot be used in a closed network environment.

Beginning with SonicOS 8.0.0, these SonicPoint devices will no longer be supported:

- SonicPoint-N
- SonicPoint-NDR
- SonicPoint-Ni/Ne
- SonicPoint-ACe/ACi/N2

What's New

- The SonicWall TZ80 offers in-product migration where you can import settings from your SonicWall SOHO/SOHOW security appliance to your new SonicWall TZ80. For more information, refer to the SonicOS 8 Migration Requirements Reference Guide.
- Beginning with SonicOS 8.0.0, support for the security protocols WEP and TKIP has been deprecated.

Known Issues

Issue ID	Issue Description
GEN8-1740	When the TZ80 X4 port is connected to a Dell Force10 switch or another SonicWall firewall in Auto Negotiate mode, the remote port is negotiated as 1G Half Duplex. **Workaround:** Manually set the X4 port into 1G Full duplex mode on both devices.
GEN8-4844	The TZ80 firmware upgrade may take up to 13 minutes before the device completely restarts. The network downtime during the upgrade will last approximately 7 minutes.
GEN8-5152	TLS displayed as **Disabled** when a LDAP server is automatically added, and displays an error if you try to manually enable TLS.
GEN8-6497	The Setup Wizard displays **Failure: "failed to finish auto-configuration"** on the summary page. After clicking OK, it will proceed, and the Setup Wizard settings are saved and take effect.
GEN8-6581	The TZ80 license expiration time is inconsistent with MySonicWall due to the time zone difference (+/- 12 hours).
GEN8-6748	When adding a network object `0.0.0.0/8`, the firewall does not display the correct net mask when saved.

Issue ID	Issue Description
GEN8-6761	User login authentication redirection starting from HTTPS URLs is not working in Chrome and Microsoft Edge browser versions 129.0.*x.x* and 130.0.*x.x*. **Workaround:** Use Firefox or any non-Chromium-based browser.
GEN8-6768	The Cloud Secure Edge (CSE) connector fails to automatically recover after an extended internet outage.
GEN8-6782	Certain switch peers, such as the Dell S4048, does not negotiate speed down on 1G on SFP links for 1000BASE-X. **Workaround:** Lower the speed explicitly to 1G.
GEN8-6817	A newly added local user may not be seen until a refresh is done.
GEN8-6833	The Wireless Clients **Configure** button is always greyed out on the **Access Point Monitor** page when managed by the TZ80.
GEN8-6864	After the TZ80 starts up, the following error is displayed: **License Manager Unavailable. The firewall can no longer communicate with the Licensing Server (LM/License Manager). Please restore**. This is a cosmetic issue and does not indicate that the device cannot contact the SonicWall License Manager service.
GEN8-6938	After Cloud Secure Edge (CSE) Tunnels have been down, it may take up to 8 minutes to get the WireGuard Session Disconnect Log even after the CES status shows a "down" status.

Additional References

GEN8-412, GEN8-5629

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 Technical Certifications
    - For Training and Assets

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 2026
Software Version - 8.2.2
232-006200-00 Rev R