SonicOS 8

Release Notes

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

Versions:

- Version 8.1.0-8017
- Version 8.0.3-8011
- Version 8.0.2-8011
- Version 8.0.1-8017
- Version 8.0.0-8037
- Version 8.0.0-8035

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.
- Firewalls currently operating on SonicOS 7.3.x, importing configuration settings is not supported.
- Firewalls currently operating on SonicOS 7.3.x are not supported for upgrade to SonicOS 8.1.x.

What's New

- **SAML 2.0 support for Generation 8 firewalls**
  SonicOS 8.1 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 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.

Version 8.1.0-8017

August 2025

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		

TZ Series	Firmware Version	NSa Series	Firmware Version
TZ680	8.1.0-8017		

This maintenance release provides fixes for previously reported issues.

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.
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.

Issue ID	Issue Description
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.

Version 8.0.3-8011

August 2025

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

TZ Series	Firmware Version	NSa Series	Firmware Version
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		

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.
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

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

Platform	Firmware Version
NSa 3800	8.0.2-8011

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.
GEN8-9866	A failure message is displayed when the reset counters are clicked in the routing rules.

Issue ID	Issue Description
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 8.1.0 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 8.1.0, enable **High Availability Stateful Synchronization**. After the firewalls are upgraded to SonicOS 8.1.0, 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

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

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.
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).

Issue ID	Issue Description
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.
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

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

Platform	Firmware Version
TZ80	8.0.0-8037

This maintenance release provides fixes for previously reported issues.

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

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

Platform	Firmware Version
TZ80	8.0.0-8035

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.

Issue ID	Issue Description
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.
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 - August 2025
Software Version - 8.1.0
232-006200-00 Rev J