

## SonicOS 7.3.2 Release Notes

These release notes provide information about these SonicWall SonicOS 7.3.2 releases:

### Versions:

- [Version 7.3.2-7010](#)
- [Version 7.3.1-7013](#)
- [Version 7.3.0-7012](#)

## Version 7.3.2-7010

March 2026

This version of SonicOS 7.3.2 is a maintenance release for existing platforms and also resolves issues found in previous releases.

## Important

- SonicOS 7.3.2 is not FIPS or Common Criteria certified.
- SonicWall firewalls running versions of SonicOS 7.1.x or later cannot be managed using Global Management System (GMS).
- Downgrading to SonicOS 7.0.x, SonicOS 7.1.x, and SonicOS 7.2.x from SonicOS 7.3.2 is not supported.
- Firewalls currently operating on SonicOS 7.3.1 (non-Hotfix) are supported for upgrade to SonicOS 7.3.2-7010.
  - ① **NOTE:** If customers have any questions or require clarification regarding the firmware upgrade path, it is strongly recommended to open a support ticket for assistance.
- Upgrading SonicOS 7.0.1 to 7.3.2 for NSv requires a fresh installation of NSv for all platforms. (For more information, refer to [NSv upgrade from 7.0.1 to 7.1.X.](#))
- Use the Firmware Auto Update feature in SonicOS 7.3.2 to ensure that your firewall always has the latest updates for critical vulnerabilities. (For more information, refer to [Firmware Auto Update.](#))

# Compatibility and Installation Notes

- A [MySonicWall](#) account is required.
- Network Security Manager (NSM) SaaS 3.5 is required to manage firewalls using SonicOS 7.3.2.
- Network Security Manager (NSM) On-Premises 3.5 is required to manage firewalls using SonicOS 7.3.2.
- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- Credential Auditor feature is not supported on NSsp 15700.

## NetExtender Compatibility & Bundling Update

- **New Version Support:** SonicOS 7.3.2 provides official support for **NetExtender version 10.3.4**, while maintaining backward compatibility with the **NetExtender version 10.2.x** branch.
- **Upgrade Recommendation:** To ensure access to the latest security patches and performance optimizations, we strongly recommend that customers upgrade all NetExtender clients to **version 10.3.4** at their earliest convenience.
- **Transition & Integration Details:**
  - **Current State:** To facilitate a seamless transition for existing users, SonicOS 7.3.2 remains embedded with **NetExtender version 10.2.341**.
  - **Future Path:** **NetExtender version 10.3.4** is scheduled to become the default embedded client in a subsequent firmware release.

## Supported Platforms

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

Platform	Firmware Version
TZ Series	7.3.2-7010
NSa Series	7.3.2-7010
NSv Series	7.3.2-7010
NSsp Series	7.3.2-7010

- |  |  |   |   |
|--|--|---|---|
| <ul style="list-style-type: none"><li>• TZ270 / TZ270W</li><li>• TZ370 / TZ370W</li><li>• TZ470 / TZ470W</li><li>• TZ570 / TZ570W</li><li>• TZ570P</li><li>• TZ670</li></ul> | <ul style="list-style-type: none"><li>• NSa 2700</li><li>• NSa 3700</li><li>• NSa 4700</li><li>• NSa 5700</li><li>• NSa 6700</li></ul> | <ul style="list-style-type: none"><li>• NSv 270</li><li>• NSv 470</li><li>• NSv 870</li></ul> | <ul style="list-style-type: none"><li>• NSsp 10700</li><li>• NSsp 11700</li><li>• NSsp 13700</li><li>• NSsp 15700</li></ul> |
|--|--|---|---|

SonicOS NSv deployments are supported on the following platforms:

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

## 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

- 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 provides security updates and resolves previously reported issues.

## Resolved Issues

Issue ID	Description
GEN7-56576	Category 14 logs are not displaying firewall system event logs in NSM.
GEN7-56535	The outbound NAT policy added for CSE connectivity is automatically deleted after a reboot. The CSE Access Tier AIPs are dynamic and are populated only after the CSE connector comes up. During device boot-up, the CSE AO remains empty, causing validation to fail and preventing the NAT policy from being added.

GEN7-56477	A certain configuration of the SSO Terminal Service Agent causes the device to reboot.
GEN7-56475	Users authenticated via SAML receive a 60-minute session duration with Google IdP
GEN7-56472	LDAP bind passwords with 14, 30, 46, and 62 characters cause the LDAP test connection and user authentication to fail due to an error in the calculation of the cipher length for an AES-256 encrypted password with PKCS#7 padding.
GEN7-56452	Some local users are showing as logged in via SAML.
GEN7-56391	Incoming IP Helper traffic from CSE GlobalEdge Access Tier is being dropped on the firewall with drop code "Packet has unallowed source IP from peer". As a result, CSE clients are unable to access any resources behind the firewall connector.
GEN7-56243	Post-authentication Format String vulnerability ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55784	Syslog is not showing the SSLVPN User login timestamp; only the SSLVPN User logout is mentioned in the report.
GEN7-55730	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55729	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55728	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55727	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55726	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55724	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55723	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55722	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55721	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55719	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55718	Unable to modify the X1 PPPoE interface on an NSM-managed firewall.
GEN7-55717	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55703	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55702	Post-authentication Stack-based Buffer Overflow ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-55581	The Session Expiry Time is miscalculated for externally authenticated guest users.
GEN7-55515	Post-authentication NULL Pointer Dereference vulnerability ( <a href="#">SNWLID-2026-0001</a> ).
GEN7-52883	In a high-availability deployment with an external Sonicwall-managed switch using a Portshield interface, the Spanning-Tree port status doesn't change on switches after HA failover.
GEN7-48603	In a high-availability deployment with an external Sonicwall-managed switch with a Portshield interface, the Spanning-Tree port status doesn't change on switches after HA failover.

## Known Issues

Issue ID	Issue Description
GEN7-54726	The IPv6 route that is added to NetExtender is incorrect when the SSLVPN IPv6 pool is a range address object.
GEN7-54715	Clicking the <b>Accept</b> button on the Geo-IP Filter settings page will enable the <b>Block all Unknown countries</b> option on the other tab automatically if nothing is configured
GEN7-54598	A locked IP address is automatically unlocked when using the GVC client. IPsec VPN reuses connection caches that are not deleted right after a login failure.
GEN7-54569	In a high-availability setup, locked-out IP addresses aren't getting synced with the standby node.
GEN7-54564	Unable to import LDAP users belonging to child domains. When clicking on Import LDAP users and selecting the primary server in the list, the user list doesn't show users from the child domain. It lists users only from the primary domain. Selecting Import from all LDAP servers will show all the users from all the servers configured/learned.
GEN7-54531	The Firewall UI is not accessible via HTTPS (port 8080) after changing from port 443. This causes a conflict. Please use a different port than 8080.
GEN7-54348	Changing the OTP length and then reverting to the original value results in the error: Ensure the minimum length is not greater than the maximum length.
GEN7-44977	CLI has commands to adjust the percentage of storage for logs, packet capture, threat-logs, and appflow-report. However, these commands have no effect because this feature was never implemented.

## Additional References

GEN7-57023, GEN7-56920, GEN7-56774, GEN7-56606, GEN7-56554, GEN7-56479, GEN7-56431, GEN7-56135, GEN7-56134, GEN7-55817, GEN7-55816, GEN7-55776, GEN7-55757, GEN7-55756, GEN7-55654, GEN7-55190, GEN7-55045, GEN7-54875, GEN7-54423, GEN7-54360, GEN7-51893

# Version 7.3.1-7013

November 2025

This version of SonicOS 7.3.1 is a maintenance release for existing platforms and also resolves issues found in previous releases.

## Important

- SonicOS 7.3.1 is not FIPS or Common Criteria certified.
- SonicWall firewalls running versions of SonicOS 7.1.x or later cannot be managed using Global Management System (GMS).
- Downgrading to SonicOS 7.0.x, SonicOS 7.1.x, and SonicOS 7.2.x from SonicOS 7.3.1 is not supported.
- Firewalls currently operating on SonicOS 7.3.0-7019 (non-Hotfix) are supported for upgrade to SonicOS 7.3.1-7013.
  - ① **NOTE:** If customers have any questions or require clarification regarding the firmware upgrade path, it is strongly recommended to open a support ticket for assistance.
- Upgrading SonicOS 7.0.1 to 7.3.1 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 7.3.1 to ensure that your firewall always has the latest updates for critical vulnerabilities. (For more information, refer to [Firmware Auto Update.](#))
- Customers using LDAP are advised to review the corresponding Knowledge Base article prior to upgrading to version 7.3.1. (For more information, refer to [LDAP Connectivity Fails After Upgrading to SonicOS 7.3.1.](#))

# Compatibility and Installation Notes

- A [MySonicWall](#) account is required.
- Network Security Manager (NSM) SaaS 3.3 is required to manage firewalls using SonicOS 7.3.1.
  - ① **NOTE:** The support for SonicOS 7.3.1 Credential Auditor feature will be available in Network Security Manager (NSM) 3.4 or higher.
- Network Security Manager (NSM) On-Premises will introduce support for SonicOS 7.3.1 beginning with Network Security Manager release 3.2.0, which is planned for availability in December.
- SonicOS 7.3.1 supports NetExtender 10.2.
- Most popular browsers are supported, but Google Chrome is preferred for the real-time graphics display on the Dashboard.
- Credential Auditor feature is not supported on NSsp 15700.

## Supported Platforms

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

Platform	Firmware Version
TZ Series	7.3.1-7013
NSa Series	7.3.1-7013
NSv Series	7.3.1-7013
NSsp Series	7.3.1-7013

- |  |  |   |   |
|--|--|---|---|
| <ul style="list-style-type: none"><li>• TZ270 / TZ270W</li><li>• TZ370 / TZ370W</li><li>• TZ470 / TZ470W</li><li>• TZ570 / TZ570W</li><li>• TZ570P</li><li>• TZ670</li></ul> | <ul style="list-style-type: none"><li>• NSa 2700</li><li>• NSa 3700</li><li>• NSa 4700</li><li>• NSa 5700</li><li>• NSa 6700</li></ul> | <ul style="list-style-type: none"><li>• NSv 270</li><li>• NSv 470</li><li>• NSv 870</li></ul> | <ul style="list-style-type: none"><li>• NSsp 10700</li><li>• NSsp 11700</li><li>• NSsp 13700</li><li>• NSsp 15700</li></ul> |
|--|--|---|---|

SonicOS NSv deployments are supported on the following platforms:

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• AWS (BYOL and PAYG)</li><li>• Microsoft Azure (BYOL)</li><li>• VMware ESXi</li></ul> | <ul style="list-style-type: none"><li>• Microsoft Hyper-V</li><li>• Linux KVM</li></ul> |
|--|---|

# What's New

- **Credential Auditor**

SonicOS 7.3.1 introduces 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.

# Resolved Issues

Issue ID	Issue Description
GEN7-55426	Device rebooting when accessing SNMP MIB <b>ipAddrTable</b> .
GEN7-55410	SAML authentication with NetExtender fails when Firefox is the default browser. After logging in, firefox downloads the SAD file instead of initiating VPN.
GEN7-55229	PPPoE is disconnecting intermittently for certain ISP providers.
GEN7-54936	Notice instability with SNMP GET request for ifTable with an illegal value of <b>0</b> .
GEN7-54896	SonicOS SSLVPN Pre-Auth Stack-Based Buffer Overflow Vulnerability (SNWLID-2025-0016).
GEN7-54855	The bandwidth Management option is missing on the <b>WAN &gt; Advanced page</b> when firewalls are in High Availability mode.
GEN7-54847	When deleting multiple users, if the deletion of any single user fails, it may cause the device to reboot.
GEN7-54843	Notice instability when using <b>http</b> in the URL to download dynamic botnet lists and dynamic external address groups .
GEN7-54817	DPI-SSL client inspection is not enforced if an IP added to DPI-SSL exclusion and removed again.
GEN7-54816	SNMP GET reports 32-bit counters for interface link speed instead of 64-bit, and incorrect speed values.
GEN7-54699	Users cannot set bandwidth management for interfaces higher than 1G.
GEN7-54597	The object disappears when creating a user or a user group whose name contains special characters under SNMP.
GEN7-54536	Connecting with NetExtender shows <b>The server is unreachable</b> due to OTP failure. The session timed out due to insufficient time for operations during the authentication process.
GEN7-52370	Displays <b>The Maximum Number of users is already logged in</b> information when trying to log in via NetExtender or Virtual Office portal to the firewall.

# Known Issues

Issue ID	Issue Description
GEN7-54716	GMS does not support SonicOS versions after SonicOS 7.0.x.
GEN7-54598	A locked IP address is automatically unlocked when using the GVC client. IPsec VPN reuses connection caches that are not deleted right after a login failure.
GEN7-54569	In a high-availability setup, locked-out IP addresses are not getting synced with the standby node.
GEN7-54564	Unable to import LDAP users belonging to child domains. When clicking on Import LDAP users and selecting the primary server from the list, the user list doesn't display users from the child domain. It lists users only from the primary domain. Selecting <b>Import from all LDAP servers</b> will display all users from all the servers configured.
GEN7-54531	The firewall UI is not accessible via HTTPS port 8080 after changing from 443, which causes a conflict. Recommended to use a different port than 8080.
GEN7-54380	With <b>New password must contain 8 characters different from the old password</b> enabled, when changing the password to something that doesn't match using NetExtender or Mobile Connect, it displays an error that may be confusing <b>Login failed - Incorrect username/password. 2 more login attempts before lockout.</b> This will be addressed in a subsequent release.
GEN7-54348	Changing the OTP Length and then changing it back results in the error: Ensure the minimum length is not greater than the maximum length.
GEN7-44977	CLI has commands to adjust the percentage of storage for logs, packet capture, threat-logs, and appflow-report. The commands have no effect as this feature was never implemented.

## Additional References

GEN7-55948, GEN7-55779, GEN7-55709, GEN7-55694, GEN7-55673, GEN7-55610, GEN7-55600, GEN7-55548, GEN7-55524, GEN7-55441, GEN7-55376, GEN7-55358, GEN7-55356, GEN7-55240, GEN7-55237, GEN7-55171, GEN7-54958, GEN7-54914, GEN7-54850, GEN7-54841, GEN7-54743, GEN7-54711, GEN7-54640, GEN7-54635, GEN7-54532, GEN7-54484, GEN7-54432, GEN7-54394, GEN7-54386, GEN7-54359, GEN7-54346, GEN7-54264, GEN7-54250, GEN7-54219, GEN7-54160, GEN7-54103, GEN7-54082, GEN7-54025, GEN7-53973, GEN7-53742, GEN7-53132, GEN7-50618.

# 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 FIPS or Common Criteria certified.
- 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, or SonicOS 7.2.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 <b>DNS Suffix</b> 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 <b>Open user's login status window in the same window rather than in a popup</b> 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: <b>Restart Required!</b> . After clicking the <b>Restart</b> button, only the Identity Provide certificate is saved. The IDP configuration will not be saved.
GEN7-53148	Unable to change the <b>Public IP Address</b> under the <b>Anti-Spam</b> settings.
GEN7-53199	When importing a Network Security Manager (NSM) template, the firewall deletes static DHCP entries.
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 <b>Traffic Shaping</b> using a certain bandwidth object, the audit module fails to find the name of the bandwidth object and the audit log displays the error <code>n.forEach is not a function</code> on the secondary firewall.
GEN7-53664	Size fields (such as the Sent and Received fields) <b>Website Accessed</b> and <b>Website Hit</b> events from the syslog are missing.

Issue ID	Issue Description
GEN7-53872	Guest WiFi users cannot access the internet when <b>Enable Policy Page without authentication</b> is enabled under <b>Guest Services</b> .
GEN7-54058	For SAML users, the <b>Members go straight to the management UI on web login</b> 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 <b>Access Point Monitor</b> page, with a wireless client to connected to the Access Point, the client <b>Allow</b> and <b>Deny</b> buttons are always grayed-out even if the ACL function is enabled or disabled.
GEN7-54348	Changing the <b>OTP Length</b> , and then changing it back, results in the error: <code>Please make sure the minimum length is not greater than the maximum length.</code>
GEN7-54354	<i>NSv series and NSsp 15700 only:</i> Users may experience a decrease in performance when configured for Policy Mode.
GEN7-54380	When <b>New password must contain 8 characters different from the old password</b> is enabled, changing the password to one that does not match when using NetExtender or Mobile Connect, an error is displayed: <code>Login failed - Incorrect username/password. 2 more login attempts before logout.</code> 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. <b>Workaround:</b> Use a different port other than 8080.
GEN7-54549	<i>TZ series only:</i> the primary storage total size is shown as 0. This should be 16 MB. The Available storage is shown correctly.
GEN7-54564	Unable to import LDAP users belonging to a child domains. When clicking on <b>Import LDAP Users</b> 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. <b>Workaround:</b> Selecting <b>Import from all LDAP servers</b> 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.

Issue ID	Issue Description
GEN7-54698	<p>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.</p> <p>Recommended Action:</p> <ul style="list-style-type: none"> <li>• <b>Option 1 (Recommended):</b> Update the primary unit's password policy to match SonicOS 7.3 defaults. See KB</li> <li>• <b>Option 2:</b> Adjust the secondary unit's policy to match the primary's existing configuration.</li> </ul> <p>Keeping password policies aligned across High Availability firewalls is essential to avoid synchronization issues.</p>
GEN7-54728	<p>A time-based one-time password (TOTP) sent by email is not sent if the local user password is too short.</p>

## 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 [Technical Certifications](#)
  - For [Training and Assets](#)

# About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOS Release Notes  
Updated - March 2026  
Software Version - 7.3.2  
232-006386-00 Rev E

Copyright © 2026 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.