SonicOS 7.1

Release Notes

These release notes provide information about the SonicWall SonicOS (SonicOS) 7 release.

Versions:

Version 7.1

December 2023

SonicOS 7.1 is a major feature release of SonicOS.

Important

The SonicOS 7.1 firmware will not be available on MySonicWall for NSsp 15700. Please contact your Service Account Manager for the firmware.

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.

What's New

- **UI Monitor and Page Enhancements**
  To help create a better user experience, enhancements have been made to the user interface.
  - There is a new tab on the **Dashboard > System** page.
  - The new **Security Services** tab provides a summary of the licensing information and detailed licensing information on each of the Security Services.

- **Tooling Support Enhancements**

  Several enhancements have been made to some diagnostics and reporting tools on the **Tech Support Report** page.

  - The layout was changed to add an **Action** section where you can download several different reports.
  - A tool tip was written for the **Download System Logs** button.
  - The System Logs file package includes event logs in CSV format.

- **SonicWave AX Support**

  This version of SonicOS integrates SonicWave 600 Series Access Points with the firewall.

- **Network Access Control Support**

  SonicOS provides APIs so that NAC vendors can pass security context to SonicOS firewalls. Using the security context SonicOS builds policies for mitigation actions, fetches dynamic user roles and other information from the NAC vendor to build information models and perform the traffic filtering. SonicOS can support multiple NAC servers from different vendors simultaneously.

- **Updates to NSv**

  With NSV Bootstrapping and Token-based Registration, this version of SonicOS simplifies mass deployments of NSv in supported cloud platforms.

  ⓘ **NOTE:** Upgrading to this version of NSv requires that you deploy a new NSv installation and import backup settings and certificates exported from your current installation. For more information, see https://www.sonicwall.com/support/knowledge-base/231208132612487.

- **Intrusion Protection Service Tuning Capabilities**

  For firewalls operating in Policy Mode, you can now selectively enable and disable specific Intrusion Protection Service rules.

- **Gateway Antivirus and Anti-Spyware Threat Profile Support**

  For firewalls operating in Policy Mode, Profile Objects support Gateway Antivirus and Anti-Spyware for Policy Enforcement

- **DNS Filtering**

  Introduces a significant update aimed at enhancing the security and efficiency of your online experience, including:

  - ***Safeguarding Against Malicious Websites:*** Proactively blocking access to known malicious domains through DNS filtering mitigates the risk of malware infections and other cyberattacks.
  - ***Enhancing Bandwidth:*** By blocking access to unnecessary or undesirable websites, it reduces bandwidth consumption and optimizes internet speeds
  - ***Filtering Inappropriate Content:*** DNS filtering delivers an additional layer of protection by blocking access to websites hosting explicit content, violence, or objectionable material.

- **Content Filtering 5.0**

  Introducing Content Filtering Engine 5.0 provides major enhancements:

  - ***Category Extension:*** Increases number and types of supported categories, resulting in improved categorization of websites.
  - ***Reputation-based blocking:*** Reputation-based URL blocking proactively identifies and blocks suspicious entities based on Reputation.
- **Active/Standby High Availability Support for SonicWall Capture Security Appliance**
- **Automatic Update Firmware Support**

  This feature simplifies the process of keeping your firewall up-to-date with the latest firmware versions, patches, and security updates.

  ⓘ | **NOTE:** This feature is not supported on NSsp 15700.
- **Ability to view Anti Spyware, Gateway Anti-Virus, and Intrusion Prevention Profile Objects**
- **Ability to store Threat/System Monitor, Audit Log, and Packet Capture files on an external storage module**

  ⓘ | **NOTE:** This feature is not supported on NSsp 15700.
- **Ability to enable Management tabs (HTTPS/PING/SSH) and Source (IP) on Interfaces.**

Resolved Issues

Issue ID	Issue Description
GEN7-15658	Packet capture is not displaying some application signatures.
GEN7-19707	Unable to disable the **Allow Geo-IP/Botnet Filter map database file upload** option.
GEN7-24864	Packet mirroring does not work for a local packet mirror.
GEN7-26633	Inbound audio for both incoming and outgoing calls is unavailable when SIP UDP frames are above certain size.
GEN7-28520	A Red or Yellow alert does not trigger the Alarm indicator on the front panel of the firewall.
GEN7-31345	SMB File transfer speed over VPN drops significantly when the files are copied to LAN device behind an NSv instance in Azure.
GEN7-31899	The configuration on the DOS policy page cannot be audited
GEN7-35181	**Synchronize Firmware** may not work as expected under some conditions.
GEN7-35248	Deleting the DHCPv6 prefix delegation for one interface will clear the prefix delegation configuration on other interfaces.
GEN7-35275	The effect of enabling **Enforce DNS Proxy For All DNS Requests** in the web management interface has been improved: If a firewall sends a DNS query itself, this kind of packets will not pass into the DNS proxy module. 2. On the **Diagnostics** page, if we add a static domain entry in static cache, and enable this option, this domain won't be resolved. but it doesn't matter if FW resolves static entry in other non-stack modules.

Issue ID	Issue Description
GEN7-36178	FTP automation fails if the server response time takes more than 2 seconds.
GEN7-37282	*TZ models, NSa2700, NSa3700, and NSv models only:* The connection cache will not correctly synchronize with the standby appliance if the Stateful Failover setting is disabled and then enabled again..
GEN7-37326	Editing the WAN GroupVPN settings and then immediately enabling or disabling WAN GroupVPN will cause some configuration settings to be lost.
GEN7-37501	After the Deny MAC-filter list containing a wireless client MAC is changed to **No MAC address** or if the deny mac-filter list has been disabled, the wireless client is still blocked.
GEN7-37511	When trying to configure the gateway when adding a policy-based route using **6to4AutoTunnel**, the error **Gateway must be default** is displayed.
GEN7-38529	With devices with a MGMT interface, the default High Availability heartbeat interface is **MGMT**. The default should be **Control HA interface**.
GEN7-38767	The SSL VPN portal cannot handle jumbo frames correctly.
GEN7-39795	The **Packet Monitor** page in not displayed when a user logs in as a system administrator.
GEN7-39850	The management interface will display the warning **Gateway must be default** when choosing an 6to4AutoTunnel interface for an IPv6 policy-based route for the gateway.
GEN7-39990	On a High Availability idle device, workload balancing operations do not get set correctly due to condition checking.
GEN7-40116	HTTPS management over Site-to-Site VPN fails when trying to use the X0 port of a NSv hosted on VMWare.
GEN7-40300	When changing the SSL-VPN client Network Address IPv4 pool, the change may not have been initiated even though it was reported as having been successful.
GEN7-40352	Adding a Content Filter Profile Objects when selecting block for **29. Search Engines and Portals** causes the error: **Command 'category "1. Violence/Hate/Racism" block' does not match.**
GEN7-40886	M-LAG/LACP does not work with Huawei Multi-chassis switches because the switch cannot manage a 132-byte LACP BPDU.
GEN7-40997	FQDN AO's used in source edited management access rules do not inherit new DNS record changes which causes stale entries to be maintained and traffic is dropped with the condition `Policy drop`. The address object table and policy table will not be properly synchronized if the hosts already exist in the address object's host list.
GEN7-41630	A disabled IPv6 VPN policy becomes enabled after being edited.
GEN7-41656	SSO enforcement shows as disabled for all zones even when there is an user-based Content Filter Service (CFS) policy.

Issue ID	Issue Description
GEN7-43151	Client loses internet access after a High Availability failover because the device receives a mismatched serial number from Capture Client, and it incorrectly considers the client as invalid.
GEN7-43386	If a VPN tunnel uses AESGCM for Phase 1 encryption, the command `show vpn tunnel` does not show the encryption and displays an incorrect PRF algorithm.
GEN7-43436	The Virtual Office portal remains accessible even when the SSL-VPN service is disabled.
GEN7-43505	Unable to add a central gateway VPN policy for DHCP over VPN when the authentication method is set to **Certificate**.
GEN7-43710	When using the web management interface to edit the WAN Group VPN, an error is displayed when the pre-shared key contains non-printable characters.
GEN7-44890	The SSL-VPN portal page cannot display the bookmark for users whose names contain an @ symbol. LDAP users that use "name@domain.com" as their display name instead of the simple "name" causes LDAP users to be unable to save bookmarks in SSL-VPN portal page.

Known Issues

Issue ID	Issue Description
GEN7-28519	Border Gateway Protocol (BGP) cannot be established when MD5 authentication is enabled.
GEN7-34246	Browser Network Time Lockout and Login Mechanism (NTLM) authentication functionality may not function as expected. **Workaround:** Users must log in to their device to authenticate.
GEN7-34484	Audit logs are cleared when the firewall is restarted.
GEN7-37742	*NSv only:* SSH login to the management console is not allowed..
GEN7-41011	Groups imported from LDAP will not be automatically filled in with the LDAP location.
GEN7-41040	A security policy is automatically added from **SSO Bypass** settings, but should not be added to firewalls configured on Policy Mode.
GEN7-41102	The **Password Change** page is not prompting for a new password when **Password change** is enabled on a firewall for an imported user.
GEN7-41340	The connected route of a sub-VLAN WAN interface turns gray when its parent interface is set to **Unassigned**.
GEN7-41593	If LACP is enabled when upgrading a High Availability pair, then High Availability should be disabled to upgrade, and each firewall must be upgraded separately.
GEN7-41996	Disabling the **Automatically adjust clock for daylight saving time** setting makes no change to the current system time.

Issue ID	Issue Description
GEN7-42202	A custom uploaded botnet signature file is not saved on the firewall and then lost when the firewall is restarted.
GEN7-43016	*VMWare ESXi UI version only:* When deploying an NSv using an `.ova` file, the error **disk image missing** is displayed. **Workaround:** 1. Unzip the `.ova` file to three files: `.vmdk` file, `.nvram` file and `.ovf` file. 2. Upload above three files to the firewall instead of the single `.ova` file.
GEN7-43049	An issue may occur intermittently when a network error is displayed in the web management interface after uploading the firmware and restarting the firewall with the factory default settings. The API sends the response and closes the HTTP connection before restarting the firewall, making it appear that the firewall is accessible.
GEN7-43500	After changing the name of a local user, the entry is still displayed in Server DPI SSL Exclusion/Inclusion lists and the user with the changed name cannot be selected.
GEN7-43554	Unable to add valid domains on **Custom Malicious Domain Name List** and **White List** pages after adding an invalid domain because the configuration change is still pending. **Workaround:** Log out of the firewall and then log in again.
GEN7-43677	The option to select the refresh rate of the Real-time Charts is not available. (The default is that the data is refreshed every 5 seconds.)
GEN7-43890	When **Enable UDP checksum enforcement** is enabled, a L2TP client cannot connect if the L2TP clients are behind NAT because in transport mode with NAT, UDP headers will have incorrect checksums due to the change of parts of the IP header during transit.
GEN7-44642	*NSsp 15700 only:* HTTPS Management using the X1 port is not accessible when the MGMT/Chassis IP and X1/Aux IP are in the same subnet.
GEN7-44690	SSL-VPN login fails to authenticate when LDAPS is configured and user tries to authenticate using CAC.
GEN7-44866	Setting the schedule for Firmware Auto Update results in an error when using the Safari web browser to administer the firewall using the web management interface.
GEN7-44892	When using **RSA Secure ID Pin with Radius** without the PIN being set, and attempting log in using NetExtender, after entering the PIN in the prompt, the Next Prompt in which the user needs to enter **PIN + SecureID** is not being displayed and the NetExtender displays the message **Login incorrect - Incorrect username/password**. **Workaround:** An administrator logs out the user. The user should be able connect successfully afterward.
GEN7-44899	DNS rules do not support address objects of type MAC or FQDN by design. Address Object Groups currently bypass this restriction.
GEN7-44909	The **Threat Logs** page does not display any data until the user clicks **Refresh**.

Issue ID	Issue Description
GEN7-45060	*TZ series only:* The firewall may restart intermittently when two SonicWave devices are connected using the built-in wireless using the mesh gateway method and the **Radio Mode** on the **Internal Wireless** Page is changed from **2.4G** to **5G mixed-80M-48**.
GEN7-45077	Clicking **Graph** on the **Access Rules** page displays **No Data** for **Used Rules** when **All** is selected for the **Since** filter.
GEN7-45081	When logged in to a firewall that is managed by Network Security Manager (NSM) and the session has expired, clicking **Config** or **Non-Config** will fail without redirecting the user to log in again.
GEN7-45110	Editing a NAC policy in an Access Rule,then changing the source address group causes an error message to be displayed: **<*address object name*> is not a reasonable value**.
GEN7-45163	The App Rule number of times matched displays zero when the application rule policy name is followed by a space.
GEN7-45194	VPN-based SD-WAN groups are displayed in the dropdown list on the **SLA Probes** page, but should be excluded.
GEN7-45207	When an LDAP server with subdomains that are added as dynamic LDAP servers, and using LDAP search for a username in the subdomain, the web management interface may become unresponsive.
GEN7-45225	When U0 is configured as Final Backup in WAN Load Balancing and X1 is not configured, the web management interface and console diagnostic pings cannot reach the internet.
GEN7-45241	An intermittent issue may occur when downloading the system log or TSR with the CPU going to 100%. **Workaround:** Disabling "Periodic secure diagnostic reporting for support purposes" on the Device > Diagnostics > Tech Support Report page is a possible workaround.
GEN7-45252	*NSsp 15700 only:* An intermittent issue occurs when the Standby firewall fails to boot from uploaded firmware with `Wrong firmware to boot` displayed in the CLI after clicking **Reboot image with current settings**. After forcing a failover on the firewall, the upgrade will complete successfully.
GEN7-45257	Bookmarks created as an LDAP user are not visible when the firewall is upgraded from SonicOS 7.0.1 to SonicOS 7.1.1.
GEN7-45303	When there are a large number of FTP-data channels (20,000), and the sessions expire in a short time interval, the caches are deleted. This can cause the firewall to have a high CPU usage and become unresponsive when handling the connection cache timer. **NOTE:** This scenario is extremely unlikely to occur, but is a current limitation of the firewall itself.

Additional References

GEN7-21050, GEN7-30510, GEN7-30873, GEN7-32613, GEN7-36401, GEN7-37384, GEN7-37924, GEN7-38708, GEN7-39004, GEN7-39068, GEN7-39249, GEN7-39837, GEN7-40176, GEN7-40351, GEN7-40379, GEN7-40499, GEN7-40657, GEN7-40659, GEN7-40662, GEN7-40738, GEN7-40780, GEN7-40803, GEN7-40913, GEN7-41276, GEN7-41658, GEN7-41967, GEN7-42015, GEN7-42120, GEN7-42230, GEN7-42246, GEN7-42417, GEN7-42425, GEN7-42545, GEN7-42955, GEN7-42956, GEN7-42964, GEN7-43124, GEN7-43319, GEN7-43448, GEN7-43732, GEN7-43774, GEN7-43799, GEN7-44083, GEN7-44255, GEN7-44281, GEN7-44538

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. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall Professional Services at https://sonicwall.com/pes.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

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 - December 2023
Software Version - 7.1
232-005888-00 Rev A