SonicWall SonicOS 7.0.1

Release Notes

These release notes provide information about the SonicWall SonicOS 7.0.1 releases.

The information for each release is listed in chronological order by release date.

Versions:

Changing the Default Password

ⓘ **IMPORTANT:** You must change the default administrator password the first time you log into your firewall or you have upgraded from a previous version of SonicOS when the default password has not been changed.

To change the default password using HTTPS management via X0:

1. Connect your management computer to the X0 interface. (DHCP addressing is available by default on the X0 port).
2. In your browser, enter the default IP address **https://192.168.168.168**.

3. When prompted, log in using these default credentials:
    - Username: `admin`
    - Password: `password`

    The change password dialog displays.
4. In the **Old Password** field, enter the default administrator password.
5. In the **New Password** field, enter your new administrator password.

    > ⓘ **IMPORTANT:** Make certain to create a password that meets the security requirements of your organization. SonicWall recommends that your password should contain at least one uppercase letter, one lowercase letter, one number, and one special character. For example `S0nicW@ll`.
6. In the **Confirm New Password** field, enter your new administrator password again.
7. Click **Change Password**.

To change the default password using the MGMT port:

1. Connect your management computer to the MGMT interface port on the appliance.
2. Configure your computer with a static IP address on the `192.168.1.0/24` subnet (such as `192.168.1.20`).
3. In your browser, enter the default IP address **https://192.168.1.254**.
4. When prompted, log in using these default credentials:
    - Username: `admin`
    - Password: `password`

    The change password dialog displays.
5. In the **Old Password** field, enter the default administrator password.
6. In the **New Password** field, enter your new administrator password.

    > ⓘ **IMPORTANT:** Make certain to create a password that meets the security requirements of your organization. SonicWall recommends that your password should contain at least one uppercase letter, one lowercase letter, one number, and one special character. For example `S0nicW@ll`.
7. In the **Confirm New Password** field, enter your new administrator password again.
8. Click **Change Password**.

Version 7.0.1-5161 July 2024

July 2024

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

ⓘ **IMPORTANT:** SonicOS 7.0.1 firmware should be only used by existing customers who are running SonicOS 7.0.1-5151 or earlier. ***Do not*** downgrade to this SonicOS 7.0.1-based firmware if you are already running a version of SonicOS 7.1.1.

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.

Supported Platforms

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

Platform	Firmware Version
TZ Series	7.0.1-5161
NSa Series	7.0.1-5161
NSv Series	7.0.1-5161
NSsp Series	7.0.1-5161

- 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

Resolved Issues

Issue ID	Issue Description
GEN7-46630	VPN traffic is intermittently dropped when specific traffic matches a route policy and security policy whose timestamp keeps changing frequently and the VPN tunnel is reset by the route table update. The recheck of the security policy causes the packet to be dropped as the traffic is determined to have been sent as clear text, but should be sent on VPN now.
GEN7-47066	The default HTTPS management NAT rule is reset to top priority after a firewall is restarted with Zero Touch enabled, overriding custom-defined NAT policies.
GEN7-48245	DPI-SSL intercepts some TLS 1.2 connections even after adding an bypass decryption policy. The decryption pre-policy lookup code attempts to identify if the Content Filtering Service (CFS) and country resolution are required to match the traffic, even when a high-priority policy with no CFS and country lookup match.
GEN7-48257	Stack-based buffer overflow vulnerability in SonicOS HTTP server (SNWLID-2024-0008)
GEN7-48274	Heap-based buffer overflow vulnerability in SonicOS SSL-VPN (SNWLID-2024-0009)
GEN7-48662	Content Filtering Service (CFS) blocking over DPI-SSL is not working when TLS hybridized Kyber support is enabled on Chrome browsers. (This support is now enabled by default on Chrome browsers.)
GEN7-48885	App Rules over DPI-SSL are not working when TLS hybridized Kyber support is enabled on Chrome browsers. (This support is now enabled by default on Chrome browsers.)
GEN7-48948	When using DPI-SSL, the block page may not be displayed.
GEN7-49425	*NSsp15700 only:* The default buffer size for a non-master blade when fetching the Geo-IP map database may experience an overflow if the database size exceeds the maximum limit.
GEN7-49544	Heap-based buffer overflow vulnerability in SonicOS IPSec (SNWLID-2024-0012)

Known Issues

Issue ID	Issue Description
GEN7-41102	The Password Change page is not prompting for a new password when **Password change** is enabled on the firewall for an imported user.
GEN7-42675	In devices configured for Policy Mode, if the highest priority matching security policy has **All** users selected, and does not have any of App/Match/URL/Web-Cat selected, then the user redirection is skipped for subsequent security policies.

Issue ID	Issue Description
GEN7-43500	After changing the name of a local user, the entry is still displayed in **Server DPI-SSL Inclusion** and **Server DPI-SSL Exclusion** lists and the user with the changed name cannot be selected.
GEN7-43554	Unable to add valid domains to the **Custom Malicious Domain Name List** and **White List** pages after adding an invalid domain because the pending configuration is still present. **Workaround:** Logging out and back in will alleviate this problem.
GEN7-46927	Traffic from a custom LAN over VPN stops when the WAN Load Balancing member order is changed.
GEN7-47528	When installing NetExtender software from the SSL VPN portal page for 32-bit Windows, the message `The installer is only for x64 machine.` is displayed .
GEN7-47918	When a lot 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 message fails.
GEN7-47948	App Rule is blocking files that do not match the hexadecimal content configured in the associated Match Object.

Additional References

GEN7-45198, GEN7-45579, GEN7-45962, GEN7-46606, GEN7-48249, GEN7-48249, GEN7-49508

Version 7.0.1-5151 March 2024

March 2024

This version of SonicOS7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5151
NSa Series	7.0.1-5151
NSv Series	7.0.1-5151
NSsp Series	7.0.1-5151

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700
- NSsp 10700
- NSsp 11700
- NSsp 13700
- NSsp 15700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

SonicOSNSv deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-42309	SonicOS SSL VPN Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability: SNWLID-2024-0005
GEN7-43727	SSL-VPN portal users are not redirected to the portal after changing their password when using RADIUS MS-CHAPv2.
GEN7-44851	The IKE proposal Authentication default value of the SonicWall Auto Provisioning Server and Client is not consistent. Default value of the SonicWallAuto Provisioning Server IKE proposal was AES-256/SHA-1 when the Server IKE proposal was AES-256/SHA-256. The SonicWall Auto Provisioning Client IKE proposal Authentication default value is now SHA1.
GEN7-44949	Cannot establish a VPN tunnel when using AESGMAC.
GEN7-44990	Garbage is printed in the `srcV6=` tag for the IPv6 system log.
GEN7-45064	New memory optimizations have been included in this build.
GEN7-45556	Unable to enable FIPS Mode in a High Availability configuration.
GEN7-45736	Duplicate records are displayed on the **AppFlow Report Users** tab.
GEN7-45797	Integer-Based Buffer Overflow Vulnerability In SonicOS via IPSec: SNWLID-2024-0004
GEN7-46209	Configuring DDNS with `dyn.com` causes the error **Network error** to be displayed in the status.
GEN7-46296	CVE-2023-48795: Prefix Truncation Attacks in SSH Specification (Terrapin Attack): SNWLID-2024-0002
GEN7-46559	DNS rebinding attack prevention is now available to be used with the DNS Proxy feature.
GEN7-46938	When trying to create an address object, there is intermittently no option to select the VPN zone.

Issue ID	Issue Description
GEN7-47372	The NetExtender version is updated to the latest release (v10.2.339). If the NetExtender client **Autoupdate** option is enabled on the **Firewall SSL VPN/Client** settings page, NetExtender clients will check for the newer version and automatically update to v10.2.339.

Additional References

GEN7-44370, GEN7-45066, GEN7-45462

Known Issues

Issue ID	Issue Description
GEN7-41102	The **Password Change** page is not prompting when **Password change** is enabled on the firewall for a Imported user.
GEN7-41996	Disabling the **Automatically adjust clock for daylight saving time** setting does not change the current system time.
GEN7-42675	In devices configured in Policy Mode, if the highest priority matching security policy has **All** users selected,, and does not have any of App/Match/URL/Web-Cat selected, the user redirection is skipped for subsequent security policies.
GEN7-43500	After changing the name of a local user, the entry is still displayed in Server DPI-SSL Exclusion and DPI-SSL Inclusion lists and the user with the changed name cannot be selected.
GEN7-43554	Unable to add valid domains on the **Custom Malicious Domain Name List** and **White List** pages after adding an invalid domain. **Workaround:** Logging out and back in should resolve the issue.
GEN7-46927	Traffic from Custom LANover VPN stops when the order of the WAN Load Balancing member is changed.
GEN7-47528	When installing the NetExtender software from the SSL VPN portal page for 32-bit Windows, the message `The installer is only for x64 machine` is displayed. **Workaround:** Download and install the NetExtender software directly from sonicwall.com.

Version 7.0.1-5145 November 2023

November 2023

This version of SonicOS7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

What's New

- Administrators can disable the Virtual Portal on the Wide Area Network (WAN) while keeping SSL VPN services unaffected. This feature offers greater control over network accessibility without disrupting secure remote connections.

  Key benefits include:

  - **Enhanced Security:** With the Virtual Portal disabled on the WAN, you can substantially reduce the attack surface for potential security breaches. External entities will not be able to access your Virtual Portals, enhancing overall network security.
  - **Uninterrupted SSL VPN Services:** By disabling the Virtual Portal on the WAN, SSL VPN services remain unaffected, ensuring that your users can continue to securely access your network resources.

  The default behavior is that the virtual portal settings are migrated from the previous SonicOS version.

  To disable the virtual portal access on the WAN Zone on the appliance:

  1. Navigate to **NETWORK | SSL VPN > Portal Settings**.
  2. In the **Portal Settings** section, enable **Disable Virtual Office on Non-LAN Interfaces**.
- Support for Non-WDS Wireless Bridge mode
- Support for AESGCM algorithms in IKEv2 for encryption

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5145
NSa Series	7.0.1-5145
NSv Series	7.0.1-5145
NSsp Series	7.0.1-5145

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700
- NSsp 10700
- NSsp 11700
- NSsp 13700
- NSsp 15700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

SonicOSNSv deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-24752	L2TP connections cannot be made when **Enable IP header checksum enforcement** is enabled. The packet is dropped for the failure to handle IPSec or an incorrect IP checksum value.
GEN7-36260	The appliance reboots with a segmentation fault after changes are made to WAN Load Balancing.
GEN7-36305	An appliance may experience high CPU usage when WAN Load Balancing is enabled.
GEN7-36796	Administrators cannot edit or disable automatically added NAT policies after **Enable the ability to disable auto-added NAT policy** is enabled on the **DEVICE | Diagnostics** page.
GEN7-37233	Users running Capture Client for MacOS may lose their Internet connection when Endpoint Security Rules are applied for SSO Enforcement.
GEN7-38094	The list of blocked countries for GeoIP is not sorted alphabetically.
GEN7-38337	Network Loop/Flood happens when enabling LACP between SonicWall and Dell switches running VLT.
GEN7-38389	Network Loop/Flood happens when enabling LACP between SonicWall and Dell switches running VLT.
GEN7-38538	Creation of a Link Aggregation Group may fail when using X0 as the aggregator interface.
GEN7-38601	The appliance displays an error and restarts when using the Access Point Floor Plan feature and managed using Network Security Manager (NSM).
GEN7-38644	Administrators cannot to filter logs based on the time.
GEN7-39035	Traffic fails after shutdown of a L2 Link Aggregation Group aggregator port (PortShield mode or trunk mode) using the management interface.

Issue ID	Issue Description
GEN7-39248	Creating an administrator account name that contains special characters causes the **Device > Settings > Firmware & Settings** page to not display any backups. The error **An error occurred but the cause could not be determined at this time** is displayed when trying to access the list.
GEN7-39415	DPI-SSL version selection options have been improved: • Removed SSL 3.0 support in the DPI- SSL version. • Provided new user interface for the **DPI-SSL version selection** on the **Diagnostics** page. • Added the corresponding diagnostic commands to the command-line interface (CLI) to match those available in the management interface.
GEN7-39523	SSL VPN users may intermittently be unable to connect with NetExtender, Mobile Connect, or Virtual Office.
GEN7-39636	*NSsp 15700 only:* When a NSsp 15700 appliance is configured in High Availability mode, the management interface may intermittently be unavailable.
GEN7-39654	The CTA (Capture Threat Assessment) Report shows IPS Reporting and Spyware Reporting as disabled when they are enabled.
GEN7-39775	Mobile client users connecting through a TZ wireless series are not able to access the internet after changing the device from WDS Station to Access point mode.
GEN7-39805	A Zero Touch session is treated as a connection going through interface X0, which blocks configuring X0 using Network Security Manager (NSM).
GEN7-40407	Using Two-Factor authentication to log in via Virtual Office when Partitions is enabled succeeds for the first domain in the dropdown list, but other domains fail displaying the error: **Incorrect name/password**.
GEN7-40455	High memory utilization may be experienced on NSv platforms.
GEN7-40534	The status code of a security policy may show as Active when the policy is disabled.
GEN7-40564	CVE-2023-2650 Possible DoS translating ASN.1 object identifiers
GEN7-40609	When logging in with the correct administrator credentials, the error **Require client certification login** is displayed when Common Access Card is enabled.
GEN7-40610	After a user has logged in using Common Access Card using a smart card, the user is shown as **Unknown User** in the **User Session** window and **Dashboard**.
GEN7-40617	Changing the web management certificate from ECDSA to RSA type does not take effect until the appliance is restarted.
GEN7-40829	*NSsp 15700 only:* The IPFix statistics are not updated after enabling IPFIX.
GEN7-40972	Loading the Geo-IP cache while loading the **Diagnostic** tab may cause high DataPlane CPU utilization.
GEN7-41026	When an appliance is configured with a value of **Any** for the service field and **Allow Management Traffic** is enabled for the access rule may cause the CPU usage to increase to 100%.
GEN7-41050	High Core 0 utilization may be seen when the appliance starts up with FQDN address objects defined.

Issue ID	Issue Description
GEN7-41064	Post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN's getBookmarkList.json URL endpoint.
GEN7-41065	Post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN's sonicflow.csv, appflowsessions.csv endpoints.
GEN7-41068	Post-authentication SSL-VPN user assertion failure leads to Stack-Based Buffer Overflow vulnerability via main.cgi.
GEN7-41069	Post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN's getPacketReplayData.json URL endpoint.
GEN7-41074	Post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN's ssoStats-s.xml, ssoStats-s.wri endpoints.
GEN7-41075	Post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN's sonicwall.exp, prefs.exp endpoints.
GEN7-41076	Post-authentication Stack-Based Buffer Overflow Vulnerability in the SSL VPN's plainprefs.exp URL endpoint.
GEN7-41107	Audit Logs configured with a field that begins with special characters (such as - or + or =) may cause memory-related issues.
GEN7-41149	*TZ series only:* Traffic may fail when setting built-in wireless on a TZ wireless model series when changing the setting from WDS station mode.
GEN7-41231	A hard-coded password was present in the `dynHandleBuyToolbar` demo function.
GEN7-41394	The information for the countries of Iraq and Syria was adjusted to no longer use DST.
GEN7-41433	improvements were made to ensure extra file system integrity checks are performed to prevent potential system corruption.
GEN7-41622	When a packet is send via VPN with certain tags, it may trigger high CPU DataPlane usage if traffic is heavy.
GEN7-41952	Post-authentication Improper Privilege Management vulnerability in the SonicOS SSL VPN Tunnel.
GEN7-43527	*NSsp 15700 only:* A High Availability Pair may show a high Core 0 utilization of 100% causing the appliance to restart.
GEN7-43528	The appliance may restart automatically after enabling LDAP authentication.

Additional References

GEN7-28433, GEN7-34477, GEN7-37004, GEN7-37288, GEN7-37318, GEN7-37858, GEN7-37943, GEN7-37977, GEN7-38521, GEN7-38795, GEN7-39183, GEN7-39401, GEN7-39443, GEN7-39522, GEN7-39876, GEN7-39937, GEN7-39958, GEN7-40001, GEN7-40046, GEN7-40051, GEN7-40073, GEN7-40232, GEN7-40370, GEN7-40660, GEN7-40737, GEN7-40779, GEN7-40781, GEN7-40798, GEN7-40908, GEN7-41521, GEN7-41644, GEN7-41730, GEN7-42178, GEN7-42199, GEN7-42952, GEN7-43153

Known Issues

Issue ID	Issue Description
GEN7-41011	Groups imported from LDAP are not automatically populated with the LDAP location.
GEN7-41040	A security policy is automatically added from the **SSO Bypass** settings, but it should not be added in appliances configured for Policy Mode.
GEN7-41102	The user is not prompted to change their password when **Password change** is enabled on the appliance for an imported user.
GEN7-41340	The connected route of sub-VLAN WAN interface displays as inactive when its parent interface is set to **Unassigned**.
GEN7-41630	An IPv6 VPN policy with a **Disabled** status will become enabled after the policy is edited.
GEN7-41996	Disabling **Automatically adjust clock for daylight saving time** makes no change to current system time.
GEN7-42202	A custom uploaded botnet signature file is not saved and then is lost when the device restarts.
GEN7-42675	In devices configured for Policy Mode, if the highest priority matching security policy has **All** users selected and does not have any of App/Match/URL/Web-Cat selected then user redirection is skipped for subsequent security policies.
GEN7-43049	An intermittent issue may occur when a network error is seen in the management interface after uploading the firmware and restating the appliance with factory default settings. The API sends the response and closes the HTTP connection before rebooting, making it appear that the unit is still operating.
GEN7-43500	After changing the name of a local user, the entry is still displayed in **Server DPI-SSL Inclusion** and **Server DPI-SSL Exclusion** lists. The user with the changed name cannot be selected.
GEN7-43505	Unable to add a central gateway VPN policy for DHCP over VPN when the authentication method is **Certificate**.
GEN7-43554	Unable to add valid domains to the **Custom Malicious Domain Name List** and **White List** page after adding an invalid domain because the pending configuration is still present. **Workaround:** Logging out and back in resolves the issue.

Version 7.0.1-5129 June 2023

June 2023

This version of SonicOS 7.0.1 (7.0.1-5129) is a maintenance release for currently shipping NSsp 15700 platforms and resolves issues found in previous releases.

Supported Platforms

ⓘ **IMPORTANT:** This release applies only to the NSsp 15700 platform.
For information about the latest release related to other platforms, please see Version 7.0.1-5119 June 2023.

Resolved Issues

Issue ID	Issue Description
GEN7-21392	The Real Time Monitor does not display all of the actual traffic going through the firewall.
GEN7-30560	Users accessing WAN from LAN using a security rule containing group Everyone displays an undetermined error when trying to change the password after logging in.
GEN7-32261	OSPFv3/RIPng]OSPFv3/RIPng cannot be established over trunked VLAN or sub-VLAN interfaces.
GEN7-33585	IPv6 VPN does not work when using a VLAN interface.
GEN7-33914	The value of OSPF interface Auto-Cost is incorrect for 40G interfaces.
GEN7-34690	The **Resolved Address** is not displayed even when the domain is resolved using the IPv6 DNS server.
GEN7-35241	If two IPv6 WAN interfaces are configured, configuring the second interface in IPv6 static mode results in the error: `Command 'dns primary xxxxx::xxx:xxxx:xxxx::xxxx' does not match`.
GEN7-36708	Unable to load a build or exp file when doing out-of-band management using the MGMT port. A different port needs to be used for out-of-band management or the system used by the administrator needs to be in the same subnet as the MGMT port.
GEN7-37068	System logs and event logs are not being processed for **Website Blocked** when Stealth Mode is enabled. The counter remains at 0.
GEN7-37135	LDAP sync fails while waiting for a reply from the LDAP server.

Issue ID	Issue Description
GEN7-37387	In an High Availability environment, the internal default OSPF route disappears from the active firewall when OSPF has been configured with LSA tracking for the default route and **default-information originate always** is selected.
GEN7-37454	Dynamic routes are deleted on Slave blades for active firewall after disabling Stateful Synchronization option. The packets are dropped due to IP Spoof check error.
GEN7-37862	Syslog packets are not generated over a VPN tunnel when two syslog servers have been enabled.
GEN7-38631	The High Availability link may not come up intermittently after upgrading the firmware.
GEN7-39016	The Arp Entry is not clear after it reaches after the counter reaches 0 minutes.
GEN7-39744	Traffic is forwarded when a security rule set to Deny/Discard in Wire Mode.
GEN7-39788	Under some conditions, the Content Filtering Service (CFS) will not block a Deny rated domain when a TCP Window Update packet is received after the connection. Instead, the policy engine will perform policy lookup processing without the URL and the ratings information.
GEN7-39993	Packets matching a Security Policy with Action Profile set to **SSO Bypass** reports `Packet Dropped - policy user sso needed` in the log. This can be a false-positive that can lead to confusion.

Additional References

GEN7-40253, GEN7-40248, GEN7-40002, GEN7-39528, GEN7-39387, GEN7-39193, GEN7-39153, GEN7-38709, GEN7-38691, GEN7-38652, GEN7-38422, GEN7-38388, GEN7-38158, GEN7-38149, GEN7-38134, GEN7-38050, GEN7-37947, GEN7-37945, GEN7-37900, GEN7-37854, GEN7-37418, GEN7-37346, GEN7-37204, GEN7-37123, GEN7-37094, GEN7-37071, GEN7-35813, GEN7-35774, GEN7-35643, GEN7-34016, GEN7-33917, GEN7-33201, GEN7-31788, GEN7-31530, GEN7-31423, GEN7-31132

Known Issues

Issue ID	Issue Description
GEN7-35781	Adding an ECMP route with tunnel VPN as the last interface fails when the **Gateway Number** is 3 or 4.
GEN7-36684	A design change now allows special management (no user policy required) only using the MGMT port on appliances that do not have a management port. For the appliances that have a management port, the user will need to add an explicit management rule to allow management service on a non-management port. Administrators must create an allow rule to allow management services using non-management ports (such as X0 and X1) and enable the corresponding management service on each of the interfaces.

Issue ID	Issue Description
GEN7-40273	Management is allowed using HTTPS/SSH through a site-to-site VPN policy when **HTTPS/SSH Management via this SA** is disabled in the VPN policy
GEN7-40300	When changing the SSLVPN client Network Address IPV4 pool, the change may intermittently not be completed even when it shows that change was successful.
GEN7-40369	An error may be displayed when clicking the **Apply** button on the **LDAP Mirror** configuration page in a High Availability configuration when a valid local certificate is removed from the firewall, but the association of the certificate is not removed from the Local TLS Certificate in the LDAP Base payload.

Version 7.0.1-5119 June 2023

June 2023

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

ⓘ **IMPORTANT:** For information about the most recent release for the NSsp 15700 platform, please see Version 7.0.1-5129 June 2023.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5119
NSa Series	7.0.1-5119
NSv Series	7.0.1-5119
NSsp Series	7.0.1-5119

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700

- NSsp 10700
- NSsp 11700
- NSsp 13700

- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670

- NSv 270
- NSv 470
- NSv 870

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

This release provides these new features:

- Event log reporting is now supported using IPFIX
- Firewall information can now be passed to Network Security Manager (NSM) through ZeroTouch heartbeat reply messages

Resolved Issues

Issue ID	Issue Description
GEN7-28162	Access points connected to the firewall failed to successfully complete.
GEN7-29806	Check Network Settings tests fail when all internet traffic is routed through VPN that is defined using an unnumbered tunnel interface.
GEN7-35191	The firewall fails to send the SFR file to Network Security Manager (NSM).
GEN7-35328	When logging in to a firewall as a read-only administrator, a warning is displayed that informs the user that they cannot preempt the existing administrator and to choose between **Do NOT Begin Management** and **Non-Config**. This is confusing because an administrator with read-only permissions should automatically start administration in non-configuration mode.
GEN7-36529	The presence of a large number of FQDN address objects can cause high CPU utilization. One effect of this is the ULA page to failing to respond for user authentication.
GEN7-36720	The firewall might automatically restart after submitting a one-time password (OTP) received by email in the NetExtender user OTP window.
GEN7-37020	The **Observed Threats Data** displayed on the Dashboard does not match the data shown in the AppFlow Report.
GEN7-37021	The front panel indicator of an interface does not indicate that it is inactive when the corresponding L2 switching LAG aggregator port becomes unavailable.
GEN7-37091	The **BWM Monitor** page displays as a blank page when there is a difference between the system time and the BWM clock time, resulting in a timeline offset in management interface display.
GEN7-37172	The **Guest Services > Custom Page** authentication does not display the custom texts or URLs.
GEN7-37403	The firewall does not accept an LDAP server name that begins with a number.

Issue ID	Issue Description
GEN7-37456	MAC filtering and options did not work as expected, including not being able to add a client to a custom allow group when the MAC filter is disabled. If an existing Address Object name was changed, clicking on the **Add** icon causes a new entry for the same MAC address to be added to the group.
GEN7-37564	A DPI-SSL server-enabled firewall is not sending server hello and server certificate packets to the client. The website times out when accessed.
GEN7-37668	On the **Network > Interfaces** page, when expanding the **Zones** field, the scaling is not working. The fields do not all move over, particularly sub-interfaces with long names.
GEN7-37693	The **Report Events via IPFIX** is missing from the system logs in current firewalls. This data was available in legacy devices .
GEN7-37763	**Capture ATP Block Until Verdict** is not blocking some file downloads. Support for Capture ATP-eligible files transferred over HTTP as gzip files was recently added..
GEN7-37994	When registering a NSv firewall, the system would report a successful registration, but did not update the licenses on the firewall.
GEN7-38129	An incorrect validation in the health check email body text causes the **Log Mail Advanced Settings** page to not function when clicking on **Advanced**.
GEN7-38156	Administrator was unable to access the management interface X0 management IP using an SSL-VPN connection over IPv6 to WAN IP on the firewall.
GEN7-38194	Disabling virtual MAC for High Availability causes the firewall to drop the ARP request generated by itself. The device could not then be managed using the WAN interface and LAN to WAN traffic would fail unless the firewall was restarted.
GEN7-38265	No audio was present when connecting with an HTML5 RDP bookmark in SSL-VPN.
GEN7-38594	A conflict between the log module and IPFIX causes the firewall to restart.
GEN7-38663	The size limit of custom header value has been adjusted to 512 characters.
GEN7-38743	Content Filtering Service (CFS) policies based on AD Groups do not work when using TSA agent for SSO authentication.
GEN7-39015	The firewall might automatically restart after submitting a one-time password (OTP) received by email in the NetExtender user OTP window.
GEN7-39024	Warnings are displayed when using DPI-SSL because of the expiration of the built-in Intermediate certificate (DigiCert SHA2 Secure Server CA).
GEN7-39347	A warning is displayed when logging in as a read-only administrator when using the MGMT interface.
GEN7-39385	The DDNS profile for `changeip.com` displays a **Network Error** warning when configuring a profile because of a change in ChangeIP's API.
GEN7-39406	The **Per Event IPFIX** control states in the Event/System Log Settings could not enabled or disabled.
GEN7-39469	The firewall may restart when an LDAP user that is part of Administrators group tries to log in to the firewall.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-39139, GEN7-38246, GEN7-38151, GEN7-37934, GEN7-37838, GEN7-37671, GEN7-37601, GEN7-37563, GEN7-37339, GEN7-37097, GEN7-37066, GEN7-36237, GEN7-34702, GEN7-32615

Known Issues

Issue ID	Issue Description
GEN7-36178	FTP automation fails if the server response takes more than 2 seconds.
GEN7-36194	If two VPN TIs are named with the same starting 16 characters, then **Advanced Routing** support cannot be enabled on both.
GEN7-37226	10G interfaces and 1G interfaces are allowed by management interface to be put into an L2 Static LAG Group even though this configuration setting should not be allowed.
GEN7-37508	When importing a configuration that has WAN to TrustZone secure WireMode interfaces configured, traffic is not blocked. The same configuration created on its own works as expected.
GEN7-39850	The warning message **gateway must be default** is displayed when choosing an 6to4AutoTunnel interface for an IPv6 Policy Based Route for the gateway.
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**.
GEN7-40390	In a NSv L3 High Availability configuration, changing the X0 IP address causes the Primary to lose its connection with Secondary. Restarting the firewall is required to to restore the connection.
GEN7-40520	After upgrading the firmware on a firewall, the firewall reports that it is not synchronized to Network Security Manager (NSM).
GEN7-40554	Importing preferences from a NSa 5600 to a NSa 6700 fails if a SSO policy are not configured correctly.

Version 7.0.1-5111 April 2023

April 2023

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

ⓘ **IMPORTANT:** For information about the most recent release for the NSsp 15700 platform, please see Version 7.0.1-5100 March 2023.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5111
NSa Series	7.0.1-5111
NSv Series	7.0.1-5111
NSsp Series	7.0.1-5111

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700
- NSsp 10700
- NSsp 11700
- NSsp 13700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

SonicOS NSv deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-29243	SNMP Queries are taking a long time to complete when there are Portshielded Interfaces and querying interface-related object identifiers.
GEN7-31345	The SMB File transfer speed over VPN drops significantly when the files are copied to a LAN device behind an NSv instance in Azure.
GEN7-32492	The OSPF MTU of Unnumbered Tunnel Interfaces is set to a fixed value of 1446, which may not always be correct.
GEN7-32624	A device may be unable to get a WAN IP from the ISP from a PPPoE connection after the device is restarted.
GEN7-33153	Appliances now require that the administrator must change the administrator password if the appliance is started from factory default settings or if the default administrator password is still `password`.
GEN7-33218	Guest users are not redirected to the captive portal authentication page.

Issue ID	Issue Description
GEN7-33655	When the user authentication method is set to RADIUS, even if the Read-Only Admins Group belongs to the user's group, the user can log in as a Full Administrator when logging in to the administration user interface using a Global VPN Client.
GEN7-34401	DHCP via IP Helper is not working over IPSec VPN in SD-WAN configurations.
GEN7-34875	*NSa 3700 only:* The appliance stops passing traffic and becomes inaccessible through the LAN interface after a few months in operation.
GEN7-35282	The download speed is slower than expected when Bandwidth Management is enabled on access rules when the TCP advertised window is not large enough.
GEN7-35355	LDAP users of the format *domain\username* are unable to authenticate when using Time-based One-Time Password authentication.
GEN7-35356	*NSa 2700 only:* An appliance may become inaccessible after being active for some time because of a deadlock state between the routing and VPN modules.
GEN7-35478	The system log displays an incorrect `fw_action` for the message `Syslog Website Accessed`.
GEN7-35530	When configuring a High Availability environment, both the Primary and Secondary device both became Active and cannot discover its peer firewall for synchronization or failover.
GEN7-35651	An option was added on the diagnostics page for GEO-IP that allows administrators to drop TCP handshakes coming from an IP address that originates from a blocked country. Synchronized packets not forwarded to the LAN Geo-IP will prevent the block page from being displayed. The default behavior if this option is not enabled requires TCP handshakes to establish a connection to be able to display the block page.
GEN7-35761	On the management user interface, the Storage LED may display as being Off, but the light remains lit on the device .
GEN7-35947	*NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, and NSsp 13700 models only:* If an administrator is logged into both the Safe Mode user interface and the Safe Mode command-line interface at the same time, and uploads firmware and restarts the appliance with the current configuration or factory default, the unit will stop responding after displaying the message `Installed Firmware`.
GEN7-36244	The management interface shows that the 10G interfaces (X29-X33) are still available in the front panel display with a TwinAX cable connected and shutting down the interfaces as an administrator.
GEN7-36461	A firewall may reboot when multiple Access Rules are deleted when the source zone is in a custom DMZ and the destination zone is a VPN.
GEN7-36535	When using a DPI-SSL server, the intermediate certificate is not being sent.
GEN7-36602	The administrator cannot disable RADIUS proxy forwarding when the user-name attribute format is set to **Other** in the SSO configuration.

Issue ID	Issue Description
GEN7-36610	Cannot to connect to WiFi when both SSID suppression and MAC filtering are enabled.
GEN7-36631	In High Availability configurations, for Flow Reporting on Network Security Manager for firewalls , the secondary device sends flow logs with the secondary serial number instead of the primary serial number.
GEN7-36703	Security Headers have been added for servers.
GEN7-36790	*NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, and NSsp 13700 models only:* An issue was intermittently experienced when an appliance could not be successfully upgraded using the Safe Mode user interface.
GEN7-36919	When using the Wizard to create a NAT policy, a Service Group gets created for service explicitly named "any" instead of using the default any Service Group.
GEN7-36965	Global VPN client RCF import fails when password contains special chars, such as `#`.
GEN7-37018	When an LDAP user without administration privileges attempts to log in from a LAN, the error message `Unknown error` is displayed instead of a more specific reason, such as `not enough privilege`.
GEN7-37044	Improper Restriction of Excessive MFA Attempts
GEN7-37095	*For TZ 270, TZ 370, and TZ 470 models only:* the **Enable Stateful Synchronization** option is not displayed within the management interface for High Availability. If this option was enabled in prior versions, the setting will continue to function even though it is not visible.
GEN7-37134	Under some conditions, the Content Filtering Service (CFS) DNS reply handling and request time can trigger conflicts in the handling of cache timers, causing the device to restart.
GEN7-37186	When CASS is enabled, the Real-time Block List (RBL) filter is not hiding the **RBL Filter** settings.
GEN7-37221	Sorting the NAT Policies list does not work as expected.
GEN7-37274	The **Send IKEv2 Cookie Notify** setting is not functioning correctly and causes establishment of a IKEv2 VPN to fail.
GEN7-37417	Deleting a user account with a domain format causes the error to be displayed: `Network Object not found`.
GEN7-37480	The QR code is blank for RADIUS users while binding SSL VPN Time-based One-Time Password (TOTP) authentication.
GEN7-37783	Devices are unable to negotiate IKE using 3rd Party Certificate VPN tunnel when using a certificate of a larger size because the DF flag forbids the fragmentation of the packet involved, causing the packet to never reach the peer gateway.
GEN7-38111	SonicOS Stack-based Buffer Overflow Vulnerability. For more information, refer to CVE-2023-0656.
GEN7-38501	A firewall with the watchdog settings enabled restarts itself every few minutes after updating to SonicOS 7.0.1-5108.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-26565, GEN7-31774, GEN7-32249, GEN7-32373, GEN7-33318, GEN7-33434, GEN7-33890, GEN7-34069, GEN7-34418, GEN7-35180, GEN7-35494, GEN7-35518, GEN7-35647, GEN7-35831, GEN7-36030, GEN7-36179, GEN7-36191, GEN7-36192, GEN7-36321, GEN7-36332, GEN7-36541, GEN7-36642, GEN7-36648, GEN7-36826, GEN7-36852, GEN7-36908, GEN7-37043, GEN7-37142, GEN7-37316, GEN7-37336, GEN7-37600, GEN7-37794, GEN7-37818, GEN7-37835, GEN7-37976, GEN7-38196, GEN7-38549, GEN7-38551

Known Issues

Issue ID	Issue Description
GEN7-35241	If two IPv6 WAN interfaces are configured, configuring the second interface in IPv6 static mode causes the error `Command 'dns primary xxxxx::xxx:xxxx:xxxx::xxxx' does not match` to be displayed
GEN7-35248	Deleting the DHCPv6 prefix delegation for one interface will clear the prefix delegation configuration on other interfaces.
GEN7-36178	FTP automation fails if the server response is longer than 2 seconds.
GEN7-36194	If two VPN tunnel interfaces are named starting with the same 16 characters, Advanced Routing support cannot be enabled on both interfaces.
GEN7-36620	*NSA 4700, NSA 5700, NSA 6700, NSsp 10700, NSsp 11700, NSsp 13700 models only:* After High Availability with Stateful Failover is set up, disabling and then re-enabling Stateful Failover, and keeping the same Control and Data interfaces, will cause the secondary unit to stay in Election state and access to the primary unit will be lost. **Workaround:** The status will recover after fifteen minutes or after the units have been power cycled..
GEN7-37226	The user interface allows 10G interfaces and 1G interfaces to be added to an L2 Static LAG Group even though this configuration is not valid.
GEN7-37326	Editing the WAN GroupVPN settings, and then immediately enabling or disabling WAN GroupVPN, may 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 remains blocked.
GEN7-37508	When importing a configuration that has WAN to TrustZone secure Wire Mode interfaces configured, the traffic is not blocked.
GEN7-37511	When configuring a gateway and adding a policy-based route using the 6to4AutoTunnel, an error is displayed: `gateway must be default.`

Version 7.0.1-5100 March 2023

March 2023

This version of SonicOS 7.0.1 (7.0.1-5100) is a maintenance release for currently shipping NSsp 15700 platforms and resolves issues found in previous releases.

Supported Platforms

ⓘ **IMPORTANT:** This release applies only to the NSsp 15700 platform.
For information about the latest release related to other platforms, please see Version 7.0.1-5111 April 2023.

Resolved Issues

Issue ID	Issue Description
GEN7-28170	Appflow Reports displays the incorrect number of threats for GAV, Anti-Spyware, Intrusion Prevention, and Applications.
GEN7-31592	Opening up a new tab by right-clicking on an existing browser tab showing **Interfaces** and then clicking **Duplicate**may display the error `Invalid authentication: SN and EPAID do not match`.
GEN7-32232	The VPN tunnel interface may periodically become inactive with IKE response packets dropped due to IKE packets from the stack not allowed in Policy Mode.
GEN7-32518	Slow transfer rates may be experienced when using TFTP.
GEN7-32882	Slow web traffic over IPSec VPN may be experienced with ESP packets dropped by the remote firewall because of an error in the checksum when the tunnel VPN is established on the slave blade of the device when management traffic is being used.
GEN7-33499	Application Security Policies may not function correctly when App Group indexes are not set correctly when objects are first created after registration.
GEN7-33612	A Guest account may be able to access the internet after the account session time has been expired
GEN7-33643	When editing the administration privilege of local users, the updates are not displayed on **Local Users** page.
GEN7-33748	When Virtual MAC is enabled, during transition from primary to backup in a High Availability configuration, the standby appliance uses the shared IP to generate ARP broadcasts.

Issue ID	Issue Description
GEN7-33848	SlowTFTP traffic may be experienced when traversing the firewall. Option ACK messages are dropped by the firewall when received on different blades than the Read Request Forward blade.
GEN7-34183	In a High Availability environment, the default routes for the directly connected interfaces are not synchronized to the secondary device.
GEN7-34397	SNMP packets are dropped with the error `NAT policy generate unique remap port failed` due to incorrect multi-blade traffic handling for SNMP traffic.
GEN7-34773	DPI-SSL may intermittently not be enforced.
GEN7-34774	The **Don't redirect unauthenticated users to log in** setting in the Action Profile object does not function as expected. Unauthenticated users are not bypassed from user-specific policies.
GEN7-35294	**Security Policy Block Page for Website Category** blocking for authenticated user displays different **Security Policies** instead of the higher- priority **Security Policy for Authenticated User Group**.
GEN7-35491	The firewall may not initiate Single Sign-on (SSO) consistently on denied websites when the Zone- based SSO is set to **Enforced**.
GEN7-35786	The sorted order of items is incorrect when sorting NAT policies by **Name**, **Created**, or **Updated**.
GEN7-35966	Single Sign-on (SSO) was not triggered for SSO enforcement before detecting that it is needed by the policies.
GEN7-36684	A design change now allows special management (no user policy required) only using the MGMT port on appliances that do not have a management port. For the appliances that have a management port, the user will need to add an explicit management rule to allow management service on a non-management port. Administrators must create an allow rule to allow management services using non-management ports (such as X0 and X1) and enable the corresponding management service on each of the interfaces.
GEN7-36980	ICMP traffic fails over a numbered tunnel interface when the packets are larger than 1472 because the remote firewall receives an incorrect checksum.
GEN7-37018	When an LDAP user without administration privileges attempts to log in from a LAN, the error message `Unknown error` is displayed instead of a more specific reason, such as `not enough privilege`.
GEN7-37069	Cannot export Security Policies to a CSV file.
GEN7-37070	Sorting NAT Policies by **Hits** and other new columns does not function as expected.
GEN7-37134	Under some conditions, Content Filtering Service (CFS) DNS reply handling and request time out ,which can trigger conflicts in the handling of cache timers and cause an unexpected restart of the appliance.
GEN7-37633	Connections fail over SSL-VPN with users using Two-Factor authentication in addition to RADIUS authentication.

Issue ID	Issue Description
GEN7-38154	SonicOS Stack-based Buffer Overflow Vulnerability. For more information, refer to CVE-2023-0656.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-24931, GEN7-27414, GEN7-28768, GEN7-29045, GEN7-29907, GEN7-31205, GEN7-31255, GEN7-31307, GEN7-31354, GEN7-31779, GEN7-32451, GEN7-32452, GEN7-32577, GEN7-33185, GEN7-33349, GEN7-33505, GEN7-33628, GEN7-33637, GEN7-33697, GEN7-33878, GEN7-34011, GEN7-34168, GEN7-34186, GEN7-34209, GEN7-34263, GEN7-34488, GEN7-34824, GEN7-34842, GEN7-34884, GEN7-34967, GEN7-35037, GEN7-35162, GEN7-35174, GEN7-35499, GEN7-35565, GEN7-35609, GEN7-35621, GEN7-35646, GEN7-35648, GEN7-35801, GEN7-35826, GEN7-35967

Known Issues

Issue ID	Issue Description
GEN7-31899	The configuration on the **DOS Policy** page cannot be edited.
GEN7-32261	OSPFv3/RIPng]OSPFv3/RIPng cannot be established over trunked VLAN or sub-VLAN interfaces.
GEN7-34690	The **Resolved Address** is not displayed when the domain is resolved when using a IPv6 DNS server.
GEN7-35781	Adding an ECMP route with Tunnel VPN as the last interface fails when the Gateway Number is either 3 or 4.
GEN7-36708	Unable to load a build or export a file when performing out-of-band management using the MGMT port. **Workaround:** Used a different port for out-of-band management or the system being used needs to be on the same subnet as the MGMT port.
GEN7-37532	The active unit in a High Availability configuration shows the same MGMT IP for both the Primary and Secondary appliances.

Version 7.0.1-5095 November 2022

November 2022

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Important

Starting with SonicOS 7.0.1-5080, the user is forced to change the default password after the first login on the following firewalls: NSa 4700, NSa 5700, NSa 6700, NSsp 10700 NSsp 11700 and NSsp 13700.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5095
NSa Series	7.0.1-5095
NSv Series	7.0.1-5095
NSsp Series	7.0.1-5095

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700
- NSsp 10700
- NSsp 11700
- NSsp 13700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

SonicOS NSv deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-26093	SSL VPN will not work if **DPI and Stateful Firewall Security** is applied before enabling SSL VPN.
GEN7-31044	A PPPoE connection will not connect until the firewall is restarted if the PPPoE connection is disconnected
GEN7-31454	Firewall discovery and SSO failure may cause users to be disconnected from the internet when authenticated through Capture Client SSO and the client is unable to reach the Sonicwall authentication servers.
GEN7-32128	A **User Login info initialization failure** error may be intermittently displayed when trying to log in to the firewall using administrator credentials.

Issue ID	Issue Description
GEN7-32179	Guest Accounts with a custom guest profile do not inherit its settings.
GEN7-32273	With X0 and X1 paired in Transparent or L2Bridge mode, firewall diagnostics are not resolving DNS names because queries are being forwarded to the wrong interface.
GEN7-32426	A FQDN that contains a hyphen cannot be used as a Syslog Server.
GEN7-32523	One-to-one loopback NAT policies are not working as expected due to policy sequence prioritization.
GEN7-32542	Using NetExtender or Mobile Connect SSL VPN, and then connecting to RDP server and launching a browser from the server, causes the SSL VPN session to be disconnected.
GEN7-32612	An **Undefined error** message is displayed when more than three values are added in one **Domain Key Pair** in the **CFS Default Profile > Custom header** field.
GEN7-32827	When upgrading from a previous version of SonicOS, the user needs to disable the port redundancy through the management user interface before upgrading the firmware on the firewall.
GEN7-32858	A general LACP issue was seen in which PORT selection was being done incorrectly upon power up of the interface - issue was seen at boot up time.
GEN7-32875	In an environment that uses Radius Accounting, and the firewall is configured to forward RADIUS Accounting requests to an unresponsive RADIUS accounting server, the CPU may reach high usage which can cause degraded performance.
GEN7-32876	In a High Availability environment, synchronization may cause NAT and Access Rules to revert to their previous settings on every failover.
GEN7-33142	In Log Automation Health Check emails, the last character in the subject line is missing.
GEN7-33156	SSL VPN connections may get saturated before the supported number of connection is reached.
GEN7-33391	An LACP member port may ungroup the aggregation after ninety seconds for 10G interfaces under certain conditions.
GEN7-33533	In a High Availability environment, frequent failovers may be seen when the peer was not receiving the heartbeat due a legacy VPN option being enabled.
GEN7-33629	A maximum of 100 devices can receive IP addresses from DHCP over VPN.
GEN7-33631	The Numbered Tunnel interface packet scheduler was not handling traffic like SQL queries properly, causing out of order packets and slow throughput over the VPN.
GEN7-33721	10G links may intermittently not be up after the a firewall is restarted.
GEN7-33847	Download speeds may be much lower when **Bandwidth Management** is enabled using access rules

Issue ID	Issue Description
GEN7-33857	Connections for Avaya Phones may be dropped across a GVC VPN because all of the available IP addresses in the VPN IP Pool are assigned. Unused IP addresses were not being freed, so the phone could not be assigned an IP address for the connection.
GEN7-33884	In **DHCP Scope Advanced Settings**, setting a **DHCP Generic Option** object with the **Option Number** as 119 (from the **DNS Domain Search List**), it is not possible to add multiple DNS suffixes in the **Option Value**.
GEN7-33915	Settings migrated from a pre-next-generation firewall may cause NAT Policies to have duplicate UUID values. The firewall will display incorrect information when the NAT policy is expanded.
GEN7-33947	Two-factor authentication may not work when a domain user tries to log into the firewall if a local non-domain user object exists that has the same name as the simple user name of the domain user.
GEN7-33981	All VPN policies are displayed as disabled if the VPN has been disabled and then re-enabled on the **Settings** tab on the **Network > IPSec VPN > Rules and Settings** page.
GEN7-34104	When Content Filtering Service (CFS) and DPI-SSL are enabled, trying to access a website using a client with a proxy enabled causesthe passphrase or confirm action not to be displayed.
GEN7-34176	The **Virtual Office** page does not display if **L3 Flood Protection** is set to **Always proxy WAN Connections**.
GEN7-34202	Pages will fail to display in the management interface if an address group is created with the name `exit`.
GEN7-34270	FTP Log automation will fail if the FTP directory name is encoded and decoded in API PUT body and GET responses.
GEN7-34478	When opening the VPN settings, the error **An error has occured but the cause could not be determined at this time.** displayed when importing a configuration that contains a tab character in the VPN name.
GEN7-34699	Migrated settings that have a trailing tab character in the **Zone** name will cause the Real-Time Charts to display no data.
GEN7-34703	The status of a redundant X1 port is displayed as **Offline** on the **Home > Dashboard > System > Device** page.
GEN7-34852	When upgrading to SonicOS 7.0.1-5080 with the current settings, the console shows displays the message **Boot up from FACTORY DEFAULT!**, but the firewall correctly restarts with the current settings.
GEN7-35233	Upgraded jQuery.
GEN7-35489	The **UDP Inactivity Timeout** value on access rules resets to 30 seconds even after being updated.
GEN7-35600	When the login is limited, a read-only or guest administrator user accessing the **Local User and Groups** page causes an error message to be displayed.

Issue ID	Issue Description
GEN7-35617	The 10G SFP High Availability interface link displays **No link** after the firewall restarts
GEN7-35690	Adding a service object with same name, but using a different case of letters as an existing service object, will cause the new service object to be auto-added to any service group to which the original object belongs.
GEN7-35769	The DNS Diagnostic does not use static DNS Proxy Cache entries when the DNS Proxy is enabled with **Enforce DNS Proxy For All DNS Requests**.
GEN7-36107	If a Deny category or URL is configured in security policy, the firewall does not send the block page to the client device.
GEN7-36188	The Firewall Management user interface and command-line interface (CLI) becomes intermittently inaccessible, but traffic continues to pass through the firewall.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-24931, GEN7-27414, GEN7-28768, GEN7-29045, GEN7-29907, GEN7-31205, GEN7-31255, GEN7-31307, GEN7-31354, GEN7-31779, GEN7-32451, GEN7-32452, GEN7-32577, GEN7-33185, GEN7-33349, GEN7-33505, GEN7-33628, GEN7-33637, GEN7-33647, GEN7-33697, GEN7-33878, GEN7-34011, GEN7-34168, GEN7-34186, GEN7-34209, GEN7-34263, GEN7-34488, GEN7-34824, GEN7-34842, GEN7-34884, GEN7-34967, GEN7-35037, GEN7-35162, GEN7-35174, GEN7-35499, GEN7-35565, GEN7-35609, GEN7-35621, GEN7-35646, GEN7-35648, GEN7-35801, GEN7-35826, GEN7-35967, GEN7-36681

Known Issues

Issue ID	Issue Description
GEN7-33905	Journal logs cannot be enabled to be persistent from within SonicOS.
GEN7-35241	If two IPv6 WAN interfaces are present, configuring the second interface in IPv6 static mode results in the error **Command 'dns primary xxxxx::xxx:xxxx:xxxx::xxxx' does not match** being displayed.
GEN7-35248	Deleting the DHCPv6 prefix delegation for one interface will clear the prefix delegation configuration on another interface.
GEN7-35285	The packet monitor drop-down packet details may display information that is not related to the packet
GEN7-35640	Traffic is not distributed as expected after a failover when using source and destination IP address binding in Round Robin-based WAN Load Balancing.
GEN7-35775	The Local CFS server **Current Using** option is always the Primary server even if the Primary is not reachable.
GEN7-35841	The **Delete items from the list** button does not work for IPS Signature/Category List objects.

Issue ID	Issue Description
GEN7-35947	When using Safe Mode upload to firmware and restart with the current configuration or factory default, the firewall will hang after displaying the message **Installed Firmware:**. (**NOTE:** This issue only affects NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, and NSsp 13700 models.) **Workaround:** • Shut down and restart the firewall to restore the configuration. • Do not log into the Safe Mode console window and the Safe Mode management user interface at the same time.
GEN7-36035	The firewall console displays **Error with HW UNIT** when starting up. **Workaround:** The messages are benign and can be ignored.
GEN7-36118	When downloading the Tech Support Report, the console displays **wlanWriteDumpToTsr cannot access**. **Workaround:** The messages are benign and the TSR is able to be downloaded.
GEN7-36178	FTP automation fails if the server response takes more than 2 seconds.
GEN7-36194	If the names of two VPN tunnel interfaces begin with the same first 16 characters, Advanced Routing support cannot be enabled on either interface.
GEN7-36244	The management interface shows that 10G interfaces (X29-X33) are still active in the front panel display with a TwinAX cable connected and shutting down the interfaces through the administration interface.
GEN7-36333	When using the command-line (CLI) instruction `import cli terminal merge best-effort`, management should not be attempted from the web management interface until the process finishes.
GEN7-36620	After High Availability with Stateful Failover is set up, disabling then re-enabling Stateful Failove, and keeping the same Control and Data interfaces, will cause the secondary unit to stay in ELECTION state and access to the primary firewall will be lost. **NOTE:** This issue only affects NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, and NSsp 13700 models.) **Workaround:** The status will recover after fifteen minutes or after the firewalls have been shut down and restarted.

Version 7.0.1-5083 September 2022

September 2022

This version of SonicOS 7.0.1 (7.0.1-5083) is a maintenance release for currently shipping NSsp 15700 platforms and resolves issues found in previous releases.

Supported Platforms

ⓘ **IMPORTANT:** This release applies only to the NSsp 15700 platform.
For information about the release related to other platforms, please see Version 7.0.1-5080 September 2022.

Resolved Issues

Issue ID	Issue Description
GEN7-29975	The ESP packet is dropped by the remote firewall because of an error in the checksum when the tunnel VPN is established on the slave blade of the device when management traffic is being used.
GEN7-30535	Changing the setting of the **Enable** checkbox for a **Syslog Server** entry may cause a full preference synchronization to the backup unit in an High Availability environment.
GEN7-30559	The firewall may automatically restart when importing a large number of LDAP users.
GEN7-30710	If an SSH session goes into configuration mode, and performs a commit for another configuration while a prior SSH session configuration commit is still in process, a deadlock state may occur.
GEN7-30858	When selecting an interface to reserve for multi-instance, the error message **Command 'reserve interface Xnn' does not match where nn = interface you want to reserve.** may be displayed. Subsequent attempts to select the interface succeed without producing the error.
GEN7-31091	**SSO via Capture Client using Endpoint Security Enforcement** login is not working when **SSO login via Endpoint Security** is enabled. The user login authentication page is displayed when accessing any website. The status of the User login session is shown as Inactive with SSO/Endpoint Security.
GEN7-31119	On the **Packet Monitor** and **Connection Monitor** pages, some of the initiator and responder routes are swapped in the display.
GEN7-31487	Synchronization of OSPF route updates from master to slave blades may fail.
GEN7-31807	Default address objects cannot be deleted for interfaces that are not assigned.
GEN7-31855	Changing the OSPF timer interval changes the authentication password and causes OSPF to stop operating.
GEN7-31911	Connectivity issues may be experienced due to inconsistencies in the OSPF route blade synchronization.
GEN7-31919	Using the boot current firmware with a local backup configuration may fail in a High Availability environment. After the firewalls restart, the configuration has not been updated.
GEN7-32062	SNMPv2 packets are being dropped as IP Spoof, but SNMPv3 packets are not.

Issue ID	Issue Description
GEN7-32096	Information sent to Analytics is reporting only one-fourth of the **Active Connections** and **App Bandwidth** than what is displayed directly in the **System Monitor** data for the firewall.
GEN7-32102	The Capture ATP scan History may intermittently disappear on a firewall in High Availability environment.
GEN7-32117	Connections may be dropped in a High Availability environment due to dynamic route blade and High Availability synchronization issues.
GEN7-32118	After failover in a High Availability environment, the secondary unit is not able to maintain OSPF adjacency with its peers and all routing entries may be lost.
GEN7-32129	After disabling source port remap under NAT, a firewall may drop traffic with the error **NAT policy generate unique remap port failed.** Traffic originating from the X0 interface works correctly for TCP, but drops with the same error for ICMP. Traffic from other interfaces or VPN do not work for TCP or ICMP. (The option was removed from multibladed platforms.)
GEN7-32197	OSPF remains in an inactive state and the Designated Router fails to initiate link-state advertisement (LSA) after failover in a High Availability environment.
GEN7-32244	Some OSPF routing entries persist even after relevant OSPF neighbor has been inactive for a period of time.
GEN7-32253	Connectivity issues may be experienced due to inconsistencies in the OSPF route blade synchronization.
GEN7-32324	Adding a chassis secondary IP on a Secondary firewall produces the error message **Chassis IP and Secondary Chassis IP overlap** ,
GEN7-32661	In a High Availabilty environment when performing Failover/Failback, that OSPF Originate Default Route may stop working.
GEN7-32691	Scheduling a backup for FTP settings may cause a file to be generated with 0 Bytes.
GEN7-32779	Configuring a static IPv6 WAN interface produces the error message **Error: Command 'dns primary 2002:4860::8888' does not match.** A condition is missing to disable the DNS fields for static WAN interfaces.
GEN7-33236	Sending TSR/Settings by FTP via Mixed Schedule did not trigger the transfer if the one-time schedule was not matched.
GEN7-33365	Nine-digit Common Vulnerabilities and Exposures (CVEs) are missing or invalid under **Object -> Profile Objects -> Intrusion Prevention -> Intrusion Prevention Objects**.
GEN7-33371	The **Factory Default Configuration** button does not function.
GEN7-33473	The **CFS Confirm/Passhrass** action does not redirect for websites that use a custom HTTP/ HTTPS port.
GEN7-33559	Information sent to Analytics is reporting only one-fourth of the **Active Connections** and **App Bandwidth** than what is displayed directly in the **System Monitor** data for the firewall.

Issue ID	Issue Description
GEN7-33630	Adding a new Security Policy fails to synchronize between the Active firewall and Standby firewall in a High Availability environment because the index value was not being returned.
GEN7-34409	NAT Lookup fails after SonicOS restarts for NAT Policy when the NAT LB probe is in a failed state because it tries to create its own Network Monitor (default) policy, but its name conflicts with an existing NetMon policy. When this occurs, the NetMon policy creation fails, causing the NAT Policy to become invalid.
GEN7-35041	The last character of syslog messages and log messages is missing.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-29143, GEN7-30911, GEN7-31421, GEN7-32097, GEN7-32874, GEN7-35723

Known Issues

Issue ID	Issue Description
GEN7-34690	The **Resolved Address** is not displayed even though the domain is resolved when using IPv6 DNS server.
GEN7-35600	When logging in with limited, read-only, or guest administrator user credentials, an error is displayed when accessing the **Local User and Groups** page.
GEN7-35640	Traffic is not distributed as expected after a failover when using source and destination IP address binding in Round Robin-based WAN Load Balancing.
GEN7-35769	DNS Diagnostic does not use static DNS Proxy Cache entries when DNS Proxy is enabled when **Enforce DNS Proxy For All DNS Requests** is enabled.
GEN7-35781	Adding an ECMP route with Tunnel VPN as the last interface fails when the **Gateway Number** is set to 3 or 4.

Version 7.0.1-5080 September 2022

September 2022

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Important

Starting with SonicOS 7.0.1-5080, the user is forced to change the default password after the first login on the following firewalls: NSa 4700, NSa 5700, NSa 6700, NSsp 10700 NSsp 11700 and NSsp 13700.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5080
NSa Series	7.0.1-5080
NSv Series	7.0.1-5080
NSsp Series	7.0.1-5080

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700
- NSsp 10700
- NSsp 11700
- NSsp 13700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

SonicOS NSv deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-28226	When using the web management interface, the values in the table in the DHCP section cannot be sorted using the column headers.
GEN7-28491	Using the special character "(" is not accepted in a VPN name.
GEN7-29640	When importing settings using the Migration Tool, Switch settings are not imported.
GEN7-30386	Group memberships set locally may not be displayed in the web management interface for an imported LDAP user associated with **Any** domain.

Issue ID	Issue Description
GEN&-30450	An LDAP user cannot change their expired password using the Virtual Office portal.
GEN7-30509	Booting uploaded firmware in a High Availability pair succeeds, but triggers an audit log that indicates that upload has failed.
GEN7-30836	When a login fails through a mobile connection on a password change that did not meet the requirements, subsequent connections will fail until the original SSL session times out.
GEN7-30874	An Aggressive mode VPN Tunnel on a DHCP WAN interface does not negotiate after the network security appliance is restarted in a WAN Load Balancing environment.
GEN7-30959	NetExtender may connect slowly and frequently disconnect when there is heavy SSL VPN usage.
GEN7-31374	When the network security appliance is restarted, a new dynamic scope from `0.0.0.1` to `0.0.0.254` is created if W0 is under **Native Bridge** mode.
GEN7-31453	Custom static routes are not automatically disabled when a WAN probe fails and goes into failover.
GEN7-31492	A High Availability state synchronization can be triggered, causing the backup unit to restart, if the requested connection uses a WAN load-balanced interface.
GEN7-31588	On the **Device > Log > Settings** page the toggle buttons to disable or apply to all categories whether a log is sent to a given resource does not work as expected.
GEN7-31660	An UDP session was being enabled for RDP sessions connected through NetExtender, causing severe packets loss and, eventually, disconnection.
GEN7-31760	Settings cannot be exported after deleting or editing a custom zone.
GEN7-31820	Link Aggregation Control Protocol (LACP) does not function as expected on interfaces above X32.
GEN7-31846	Configuring Bandwidth Management and using **Tunnel All** mode in SSL VPN may degrade throughput on the network security appliance.
GEN7-31850	Custom Routes on the WAN are not disabled when the WAN Logical Probes Fail in a WAN Load Balancing setup.
GEN7-31884	If more than one login to the command-line interface (CLI) using SSH is attempted simultaneously when using RADIUS, LDAP, or TACACS+ authentication, the user groups list may no longer be valid after the first authentication is completed. This condition may cause a disruption of network traffic and loss of access to the web management interface.
GEN7-31900	Configuration changes on the **DoS Action Profile** page are not listed in the log files and cannot be audited.
GEN7-31907	Some third-party switches may have different default configurations for 1000BASE-X auto-negotiation without the option to bypass auto- negotiation, which may cause the connection to SonicWall to fail.

Issue ID	Issue Description
GEN7-31909	The **User Status** page does not display the active Terminal Services Agent (TSA) identified users.
GEN7-32311	DPI-SSL does not works properly when an interface is in Layer 2 bridge mode and when the **Never route traffic on this bridge-pair** option is disabled.
GEN7-32325	The SSL VPN portal displays multiple domains incorrectly in the drop-down list.
GEN7-32331	With the maximum number of SSH sessions established and new sessions being attempted, the SSH daemon thread and web server may stop working if a change to the interface or a similar event occurred at the same time.
GEN7-32338	The SonicWall DHCP server does not handle DHCP Relay Information Option (option 82) in the DHCP relay.
GEN7-32347	A SNMP get of `getDeviceInfo` returns an invalid object identifier.
GEN7-32348	A network security appliance may restart in a High Availability environment with a very large number of active users.
GEN7-32349	A buffer underrun in the DP-engine might be seen in the **Topology** section of the web management interface.
GEN7-32549	After an upgrade to the firmware, the SSL Server certificate may not be imported, causing the DPI-SSL server to stop working.
GEN7-32578	Administrators may be unable to edit the **Log Automation** page when using a mixed schedule object.
GEN7-32602	DNS packets may be dropped when UDP Flood Protection is running.
GEN7-32667	After restoring the backup configuration, the WLAN PSK passphrase cannot be changed, displaying the error message: `WLAN authentication type: Invalid`.
GEN7-32718	The settings of a WPA-state machine can become corrupted if a group key renewal occurs during an unscheduled update window. Wireless users may be unable to connect after the schedule is reactivated.
GEN7-33058	On the **Users > Settings** page, on the **User Sessions** tab, configuring **For other unidentified connections** to **Log user name** with a value that is 8 multiples of the value may cause an overrun.
GEN7-33083	SNMP monitoring may not operate for secondary WAN interfaces.
GEN7-33237	After importing settings, administrators may not be able to disable PortShield, resulting in the error: Failed: `Disabled PortShield port cannot be switched out of PortShield`.
GEN7-33361	Forcing the speed of a 1G Copper port may cause link up issues.
GEN7-33489	Forcing the speed of a 1G Copper port may cause link up issues.
GEN7-34407	When a storage module is replaced, the firewall fails to start up and displays a fatal error.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-5535, GEN7-19446, GEN7-23006, GEN7-24617, GEN7-24696, GEN7-24950, GEN7-25844, GEN7-26264, GEN7-26321, GEN7-26806, GEN7-27200, GEN7-27511, GEN7-28004, GEN7-28117, GEN7-28405, GEN7-28691, GEN7-28771, GEN7-28781, GEN7-28804, GEN7-29052, GEN7-29255, GEN7-29354, GEN7-29357, GEN7-29377, GEN7-29416, GEN7-29612, GEN7-29647, GEN7-29832, GEN7-30328, GEN7-30365, GEN7-30446, GEN7-30451, GEN7-30474, GEN7-30480, GEN7-30508, GEN7-30536, GEN7-30587, GEN7-30617, GEN7-30677, GEN7-30678, GEN7-30695, GEN7-30697, GEN7-30823, GEN7-30876, GEN7-30888, GEN7-30890, GEN7-31017, GEN7-31035, GEN7-31045, GEN7-31072, GEN7-31111, GEN7-31130, GEN7-31220, GEN7-31225, GEN7-31226, GEN7-31239, GEN7-31246, GEN7-31259, GEN7-31270, GEN7-31290, GEN7-31314, GEN7-31316, GEN7-31331, GEN7-31371, GEN7-31485, GEN7-31604, GEN7-31608, GEN7-31611, GEN7-31617, GEN7-31683, GEN7-31687, GEN7-31769, GEN7-31772, GEN7-31776, GEN7-31848, GEN7-31851, GEN7-31906, GEN7-31953, GEN7-31989, GEN7-32053, GEN7-32101, GEN7-32107, GEN7-32116, GEN7-32153, GEN7-32158, GEN7-32250, GEN7-32381

Known Issues

Issue ID	Issue Description
GEN7-33502	The Local and Peer IKE ID cannot be deleted on an IPv4 or IPv6 VPN policy
GEN7-33585	IPv6 VPN is not working when on a VLAN interface.
GEN7-33850	PPPoE IPv6 WAN traffic may drop because IPV6 NDP entries are not getting updated. **Workaround:** Restart the network security appliance.
GEN7-33981	Disabling and then re-enabling the **Enable VPN** setting on the **Settings** tab on the **Network > IPSec VPN > Rules and Settings** page results in all VPN policies being shown as disabled.
GEN7-34391	A client system may be unable to obtain a IPv6 address from a DHCP v6 Server through the IP-Helper relay policy.

Version 7.0.1-5072 June 2022

June 2022

This version of SonicOS7.0.1 (7.0.1-5072) is a maintenance release for currently shipping NSsp 15700 platform and resolves issues found in previous releases.

Supported Platforms

ⓘ **IMPORTANT:** This release applies only to the NSsp 15700 platform.
For information about the release related to other platforms, please see Version 7.0.1-5065 April 2022.

Resolved Issues

Issue ID	Issue Description
GEN7-28720	The Application Bandwidth Monitor may not report the full set of statistics.
GEN7-29262	Traffic may fail to pass through the VPN tunnel interface for tunnel VPN policies established on non-master blades when the VPN is bound to a VLAN and parent interface of the VLAN is unassigned.
GEN7-29777	The web management interface may refresh very slowly when the **User Group** page contains more than 2800 user groups.
GEN7-30009	The **Security Policies** page may display **No Data** briefly when loading more than 600 entries.
GEN7-30412	On the **Users Status** page, the **Inactivity Remaining** column may not display properly on the **Users** list.
GEN7-30459	On **LDAP User Import** page, only the first **LDAP Group** displays any users when user groups are read from the **LDAP Server**.
GEN7-30599	Unnecessary warning of the lock `gBkupTaskMutex` is displayed on console for `tRemoteBackupd`.
GEN7-30786	In the web management interface, administrators cannot browse through the full list of NAT policies.
GEN7-30787	Users are displayed as being inactive when traffic sourced from a user IP is crossing the network security appliance when SSO agent, TSA, or NTLM are enabled.
GEN7-30789	A crash may be encountered on the primary network security appliance after disabling High Availability because of attempting to synchronize an SSO failure report to the master blade.
GEN7-31032	The error **Cannot read property 'id' of undefined** displays when adding a custom match object.
GEN7-31138	After a stateful High Availability failover, traffic may be interrupted for more than 10 seconds due to G-ARP not being captured on the client host system.
GEN7-31262	The Content Filtering Service (CFS) server is not reachable from a standby unit in a High Availability pair because the request was not using the monitoring IP address of its related interface.
GEN7-31289	In a High Availability pair, the secondary unit may reboot due to settings becoming unsynchronized after clearing packet capture.

Issue ID	Issue Description
GEN7-31388	In a High Availability configuration, and both Primary and Secondary Chassis IPs are configured, when the Primary firewall is removed from the High Availability mode, an error about IP overlap is displayed after pressing OK on the management interface settings screen.
GEN7-31425	In a High Availability configuration, with IPHelper enabled and the resolution set to **DNS then NetBios**, a Failover can eventually occur on the primary device, but remain stable on the secondary device.
GEN7-31625	In a High Availability configuration, the primary unit's VLAN interface MAC address of a static LAG pair is being published also from the secondary unit's secondary LAG interface into the directly connected switch port, displaying an error during setup: **evpn duplicate mac dampening detected**.
GEN7-31636	The **Real-Time Monitor** on the **System Monitor** tab may display gaps in the graphs of **Multicore Monitor**.
GEN7-31803	SonicOS shuts down and reboots due to a segmentation fault.
GEN7-31805	Stateful Synchronization requires 40 minutes to be ready after the Control Interface is unplugged or plugged in, resulting from the retransmission of High Availability settings synchronization having too many duplicate synchronization packets
GEN7-31835	Enabling packet capture on the primary unit in a High Availability pair may trigger a segmentation fault and the secondary unit becomes stuck in High Availability synchronization mode even though the primary unit was rebooting.
GEN7-31931	In a High Availability configuration, the primary device may reboot while synchronizing the DHCP binding.
GEN7-32023	Using packet capture or diagnostic tools on the primary unit in a High Availability pair triggers a synchronization of the settings.
GEN7-32032	Importing settings may cause a lock issue on the **Policy** table.
GEN7-32163	Some decryption policies are missing, and the order of the policies is changed, upon failover from a primary unit to a secondary unit in a High Availability pair.
GEN7-32540	A crash may be seen with a stacktrace for `DP-engine-0` in a High Availability Pair causing failover when running a heavy load of mixed traffic, UDP traffic, and OSPF routes when DPI-SSL Decryption Policies and Bandwidth Management are configured.
GEN7-32620	A crash may be seen with a stacktrace for `delayedLog.c` in a High Availability Pair causing failover when running a heavy load of mixed traffic, UDP traffic, and OSPF routes when DPI-SSL Decrytion Policies and Bandwidth Management are configured.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-32314, GEN7-32297, GEN7-32215, GEN7-32192, GEN7-31905, GEN7-31849, GEN7-31297, GEN7-31272, GEN7-30337, GEN7-30082, GEN7-30054, GEN7-29178

Known Issues

Issue ID	Issue Description
GEN7-31899	The configurations on the DOS policy page cannot be audited.
GEN7-32179	Guest Accounts with a custom guest profile do not inherit its settings.
GEN7-32261	OSPFv3/RIPng cannot be established over trunked VLAN or sub-VLAN interfaces.

Version 7.0.1-5030-R945 May 2022

May 2022

This version of SonicOS7.0.1 (7.0.1-5030-R945) is a maintenance release for currently shipping NSsp 15700 platform and resolves issues found in previous releases.

Supported Platforms

ⓘ **IMPORTANT:** This release applies only to the NSsp 15700 platform.
For information about the release related to other platforms, please see Version 7.0.1-5030 December/October 2021.

Resolved Issues

Issue ID	Issue Description
GEN7-29058	A wildcard FQDN object will not resolve subdomains unless a *www* FQDN object is also created.
GEN7-29777	The web management interface may refresh very slowly when the **User Group** page contains more than 2800 user groups.

Issue ID	Issue Description
GEN7-29262	Traffic may fail to pass through the VPN tunnel interface for tunnel VPN policies established on non-master blades when the VPN is bound to a VLAN and parent interface of the VLAN is unassigned.
GEN7-30021	Incorrect IPv6 addresses are displayed for logged-in users on the **User Status** page.
GEN7-30065	Trying to manually log out users in the web management interface after they are populated and active displays the error: **command 'killuser ...' does not match**.
GEN7-30459	On **LDAP User Import** page, only the first **LDAP Group** displays any users when user groups are read from the **LDAP Server**.
GEN7-30599	Unnecessary warning of the lock `gBkupTaskMutex` is displayed on console for `tRemoteBackupd`.
GEN7-30681	The packet monitor settings on the standby firewall display the primary configuration instead of the runtime configuration.
GEN7-30716	When importing settings for High Availability the error **Failed to create cloned ifList** is displayed because of a synchronization issue .
GEN7-30743	The network security appliance may reboot when a command-line interface (CLI) stage was destroyed unexpectedly when accessing data.
GEN7-30786	In the web management interface, administrators cannot browse through the full list of NAT policies.
GEN7-30787	Users are displayed as being inactive when traffic sourced from a user IP is crossing the network security appliance when SSO agent, TSA, or NTLM are enabled.
GEN7-30789	A crash may be encountered on the primary network security appliance after disabling High Availability because of attempting to synchronize an SSO failure report to the master blade.
GEN7-31032	The error **Cannot read property 'id' of undefined** displays when adding a custom match object.
GEN7-31244	When trying to create decryption policy using an LDAP imported group, the error **Cannot read properties of undefined (reading 'success')** is displayed.
GEN7-31260	The network security appliance may reboot when TSR is pulled on units in High Availability.
GEN7-31262	The Content Filtering Service (CFS) server is not reachable from a standby unit in a High Availability pair because the request was not using the monitoring IP address of its related interface.
GEN7-31289	In a High Availability pair, the secondary unit may reboot due to settings becoming unsynchronized after clearing packet capture.
GEN7-31625	In a High Availability pair, the primary unit's VLAN interface MAC address of a static LAG pair is being published also from the secondary unit's secondary LAG interface into the directly connected switch port, displaying an error during setup: **evpn duplicate mac dampening detected**.

Issue ID	Issue Description
GEN7-31803	SonicOS shuts down and reboots due to a segmentation fault.
GEN7-31805	Stateful Synchronization requires 40 minutes to be ready after the Control Interface is unplugged or plugged in, resulting from the retransmission of High Availability settings synchronization having too many duplicate synchronization packets
GEN7-31835	Enabling packet capture on the primary unit in a High Availability pair may trigger a segmentation fault and the secondary unit becomes stuck in High Availability synchronization mode even though the primary unit was rebooting.
GEN7-31889	Stack-based buffer overflow in SonicOS potentially resulting in Denial-of-Service (DoS).
GEN7-31890	Potential exposure of sensitive information to an unauthorized user via SNMP.
GEN7-31990	Potential exposure of Wireless Access Point (WAP) sensitive information via SNMP.
GEN7-31991	Improper restriction of TCP communication channel potentially resulting in Denial-of-Service (DoS).
GEN7-31992	Allocation of resources without limits or throttling can potentially result in HTTP DoS via the Content Filtering Service (CFS).
GEN7-31994	Unnecessary `tNetObjMgr` stack traces are displayed on the console.
GEN7-32023	Using packet capture or diagnostic tools on the primary unit in a High Availability pair triggers a synchronization of the settings.
GEN7-32163	Some decryption policies are missing, and the order of the policies is changed, upon failover from a primary unit to a secondary unit in a High Availability pair.
GEN7-32418	The OpenSSL library can enter an infinite loop when parsing an invalid certificate, potentially resulting in Denial-of-Service (DoS).
GEN7-32540	A crash may be seen with a stacktrace for `DP-engine-0` in a High Availability Pair causing failover when running a heavy load of mixed traffic, UDP traffic, and OSPF routes when DPI-SSL Decryption Policies and Bandwidth Management are configured.
GEN7-32620	A crash may be seen with a stacktrace for `delayedLog.c` in a High Availability Pair causing failover when running a heavy load of mixed traffic, UDP traffic, and OSPF routes when DPI-SSL Decrytion Policies and Bandwidth Management are configured.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-32215, GEN7-32032, GEN7-31993, GEN7-31953, GEN7-31931, GEN7-31803, GEN7-31636, GEN7-31297, GEN7-30536, GEN7-28170

Known Issues

Issue ID	Issue Description
GEN7-30509	Booting uploaded firmware in a High Availability pair succeeds, but triggers an audit log that indicates that upload has failed.
GEN7-30559	The network security appliance may reboot when importing of a large number of LDAP users.
GEN7-31119	On the **Packet Monitor** and **Connection Monitor** pages, some initiator and responder routes are getting swapped in the display.
GEN7-31421	There is a maximum string length of 100 characters for the input fields for the source and destination addresses within the **Monitor Filter** tab for packet capturing. This is not enough characters to allow up to ten IP addresses to be entered in those fields as described in the informational tip.
GEN7-32518	Slow throughput may be experienced during TFTP.

Version 7.0.1-5065 April 2022

April 2022

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5065
NSa Series	7.0.1-5065
NSv Series	7.0.1-5065
NSsp Series	7.0.1-5065

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700
- NSsp 10700
- NSsp 11700
- NSsp 13700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

SonicOS NSv deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-19015	Cannot connect to Layer Two Tunneling Protocol (L2TP) with packets dropped as the packet does not match traffic selectors if the L2TP clients are behind a network address translation (NAT) IP address assignment.
GEN7-19520	An error may be displayed when accessing the Topology view when a large number of client systems are connected.
GEN7-24141	New devices may not be acquired by Network Security Manager (NSM) that have settings for VoIP are imported from an older (pre-2020) device.
GEN7-26188	The LED for LAN bypass does not work as expected.
GEN7-26488	Native Bridge Mode Pair causes IP traffic drops from and between the paired VLAN interfaces and causes the firewall web management interface to become inaccessible.
GEN7-26726	Purge option to delete log files from storage cannot be selected if two or more files are selected.
GEN7-28690	In a High Availability configuration, a reboot may be seen due to a segmentation fault in `DP-engine-1`.
GEN7-28776	The **Virtual Office Bookmark** tab is not visible when a **MGMT-Only** privilege is added to the **SSLVPN Services** group by adding a group, enabling **Members go straight to the management UI on web login**, and then removing the new group.
GEN7-28888	An SNMP query fails over a site-to-site VPN when network address translation (NAT) is enabled.
GEN7-29012	When using external storage, the system logs file location changes from secondary storage to primary storage after the network security appliance is rebooted.
GEN7-29058	A wildcard FQDN object will not resolve subdomains unless a www FQDN object is also created.
GEN7-29162	When using migrated settings, the **Path Selection Profile** interface status displays **Not Qualified** for **SD-WAN Group** interfaces when using the default SLA class object.
GEN7-29210	Unable to add 10 GB SFP+ interfaces for Port Mirroring.

Issue ID	Issue Description
GEN7-29376	SonicWall Switches managed using a network security appliance and connected on a Trunk port are not receiving a DHCP IP address from its native Interface.
GEN7-29535	Console prints `tTimerTask` stacktrace about every 1 hour. There is no functional effect.
GEN7-29547	Slow response times may be experienced when accessing a RDP session using a Virtual Office bookmark.
GEN7-29552	Unbinding the Time-based one-time password (TOTP) key from the **User Login Status** page did not work if the user password does not meet the complexity constraints.
GEN7-29603	A WAN Group VPN shared secret is displayed incorrectly when administering the network security appliance using Network Security Manager (NSM).
GEN7-29650	When trying to set up Quota limit for Radius or LDAP users, the message **script is missing one or more "exit" commands** may be displayed.
GEN7-29853	Settings are not saved when importing LDAP users and assigning the user quota on the **Import** page.
GEN7-29867	Trying to add an **All Deny** access rule on the **WAN > WAN** page maybe display the error **Rule Blocks Management Rule(s)**.
GEN7-29872	**Server DPI-SSL**, the error message **The server is not sending intermediate certificate** may be displayed.
GEN7-29904	The **Test** LED is not blinking on the Standby unit in a High Availability pair.
GEN7-29990	The RDP SSL VPN Virtual Office bookmark setting **Automatically login, Use SSL-VPN account credentials** has been removed due to security concerns.
GEN7-30015	TCP traffic fails to pass through the WAN zone native bridge interfaces when the destination IP address is not in the same subnet with the client system.
GEN7-30040	Allocation of resources without limits or throttling can potentially result in HTTP DoS via the Content Filtering Service (CFS).
GEN7-30063	When a Guest user is included in a group membership of "Guest Administrator": The message **Auto- Generate password" feature for isn't working according to the assigned Guest profile** may be displayed. When trying to export the user list, the button does not work. When using the **Print** icon, the password is not displayed on the paper.
GEN7-30334	When saving the configuration of an LDAP user in **Local Users & Groups**, the message **script is missing one or more "exit" command** might be displayed.
GEN7-30418	Not able to change the **Default target IP** under **WAN failover and Load balancing Probe** settings if using `0.0.0.0`.
GEN7-30590	Importing settings fail and trigger a trace indicating a post file HTTP issue through the API.
GEN7-30620	The **VPN** category is missing from the **Category** list in **Application Control** when trying enable a block for the **VPN** category.

Issue ID	Issue Description
GEN7-30681	The packet monitor settings on the standby firewall display the primary configuration instead of the runtime configuration.
GEN7-30698	The **Local User** display can be very slow to refresh. Searching for local users causes the **Local Users** interface to become unresponsive when a large number of configured users are present.
GEN7-30716	When importing settings for High Availability, the error **Failed to create cloned ifList** is displayed because of a synchronization issue .
GEN7-30743	The network security appliance may reboot when a command-line interface (CLI) stage was destroyed unexpectedly while accessing data.
GEN7-31049	When the **Trusted Relay Agent Check** is enabled, the Global VPN Client (GVC) client may become unresponsive in **Acquiring IP** status and the firewall fails to offer DHCP IP addresses.
GEN7-31069	The SNMP Manager may be unable to get responses from an idle firewall in a High Availability pair over a VPN.
GEN7-31215	The **Suppress Automatic Access Rules Creation** for a VPN Policy is not available.
GEN7-31244	When trying to create decryption policy using an LDAP imported group, the error **Cannot read properties of undefined (reading 'success')** is displayed.
GEN7-31260	The network security appliance may reboot when TSR is pulled on units in High Availability.
GEN7-31313	In WAN Load Balancing, the default gateway cannot be used as the default target IP address when all targets are set to `0.0.0.0`.
GEN7-31334	Log files stored on external storage cannot be deleted.
GEN7-31358	*NSA 6700 only*: The LACP configuration fails on the 40GB Interface (X33).
GEN7-31361	Unable to add or edit an WLAN interface when **Only allow traffic generated by a SonicPoint/SonicWave** is disabled. The error **Command 'no auto-discovery' does not match** is displayed.
GEN7-31420	When the rendering of the BGP neighbor status exceeds approximately 32k bytes, the **Settings** page does not display correctly.
GEN7-31746	Enabling **Mirror LDAP user groups locally** does not display the imported mirrored groups.
GEN7-31987	Potential exposure of Wireless Access Point (WAP) sensitive information via SNMP.
GEN7-31988	Potential exposure of sensitive information to an unauthorized user via SNMP.
GEN7-32041	When **AppFlow** is enabled, CP core usage will spike and many fields report that CP core CPU usage remains at 100% for an extended period of time.
GEN7-32225	The OpenSSL library can enter an infinite loop when parsing an invalid certificate, potentially resulting in Denial-of-Service (DoS).

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-19015, GEN7-19520, GEN7-24141, GEN7-26188, GEN7-26488, GEN7-26726, GEN7-28690, GEN7-28776, GEN7-28888, GEN7-29012, GEN7-29058, GEN7-29162, GEN7-29210, GEN7-29376, GEN7-29535, GEN7-29547, GEN7-29552, GEN7-29603, GEN7-29650, GEN7-29853, GEN7-29867, GEN7-29872, GEN7-29904, GEN7-29990, GEN7-30015, GEN7-30040, GEN7-30063, GEN7-30334, GEN7-30418, GEN7-30590, GEN7-30620, GEN7-30681, GEN7-30698, GEN7-30716, GEN7-30743, GEN7-31049, GEN7-31069, GEN7-31215, GEN7-31244, GEN7-31260, GEN7-31313, GEN7-31334, GEN7-31358, GEN7-31361, GEN7-31420, GEN7-31746, GEN7-32041

Known Issues

Issue ID	Issue Description
GEN7-31588	On the **Device > Log > Settings** page the toggle buttons to disable or apply to all categories whether a log is sent to a given resource does not work as expected.
GEN7-31724	When using a custom authentication partition, it displays a user in the **Unauthenticated Users** list. If the partition is disabled or using the default authentication partition, it displays the user on the **Active Users** list.
GEN7-31820	Link Aggregation Control Protocol (LACP) does not function as expected on interfaces above X32.
GEN7-31926	A SonicWall Switch becomes unreachable after its DHCP lease expires when added to a **Dedicated Uplink** topology.
GEN7-32258	When the MSSP license is expired, the network security appliance always prompts that the system needs to restart.
GEN7-32311	DPI-SSL does not works properly when an interface is in Layer 2 bridge mode and when the **Never route traffic on this bridge-pair** option is disabled.
GEN7-32411	Network Security Manager (NSM) reports that the network security appliance is unregistered in MSSP mode, even when appliance is registered.
GEN7-32602	DNS packets may be dropped when UDP Flood Protection is running.
GEN7-32696	As an administrator, closing the aggregator port in a L2 Link Aggregation Group (LAG) which uses DHCP causes traffic to fail to pass through.A

Version 7.0.1-5054 April 2022

April 2022

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Supported Platforms

ⓘ **IMPORTANT:** This release applies only to the NSsp 15700 platform.
For information about the release related to other platforms, please see Version 7.0.1-5052 April 2022.

Resolved Issues

Issue ID	Issue Description
GEN7-19536	A 10Gbps link between SFP+ ports and SWS14-48 Switches connectivity is not working when the interface speed is configured to 10Gig Full Duplex. **Workaround:** Configure the SFP+ interface and SWS14-48 Switch SFP+ interface speed to 1000Mbps Full Duplex
GEN7-28338	Several IPv6 SSO inefficiencies in the mechanism for inter-blade user synchronization requests (those which request other blades to send something back, and then wait for the response) have been resolved.
GEN7-28475	The web management interface reports **Command xxx did not match** when the guest service is enabled on the LAN zone and the same IP address is used for both administrators and guests to manage the management interface.
GEN7-29412	The web management interface does not display the interface status indicators on the front panel widget of the Dashboard on when it is first accessed.
GEN7-29415	The VLAN subinterface does not display the correct MTU in the web management interface when Jumbo frames are enabled.
GEN7-29590	An intermittent crash might be seen when adding SSO users through a third-party API and IPv6 and IPv4 groups overlap while IPv4/IPv6 traffic is present.
GEN7-29592	Blade mismatch warnings are displayed for SSO API user authentication with large number of users.
GEN7-29593	A memory leak may occur from the SSO API, when returning multiple errors in response to an SSO API request with multiple users.
GEN7-29623	In L3 Port Aggregation, the **Aggregate Port** does not display the correct link state on the **Dashboard** page of the web management interface.

Issue ID	Issue Description
GEN7-30021	Incorrect IPv6 addresses are displayed for logged in users on the **User Status** page.
GEN7-30043	Warnings are displayed on the console relating to holding locks/semaphore for a long time.
GEN7-30065	Trying to manually log out users using the web management interface once they are populated and active displays the error: **command 'killuser ...' does not match**.
GEN7-30332	A crash may be observed when accessing the IPv6 address cache with a mix of IPv4 and IPv6 users being repeatedly logged in or out,
GEN7-30390	The maximum number of VLANs that could be displayed was previously set to 24. This has been Increased it to display a maximum number of 1024 VLANs.
GEN7-30456	Audit Logging stops reporting Security Policy action profile changes when an UPE policy is configured with specific match criteria.
GEN7-30558	In High Availability, for Standby firewall, the route policies of VLAN interfaces (whose physical interface is configured as LAG) are in wrong status when link is turned off or on.
GEN7-30586	After enabling **Mirror LDAP user groups locally**, the web management interface does not display the imported mirrored groups.
GEN7-30708	Unnecessary shadow policy-related tracebacks are being reported on the Standby firewall.
GEN7-30709	After rebooting a unit in a High Availability pair, all users were being flushed from the unit's slave blades right after they were synchronized to them from its master blade.
GEN7-30710	If an SSH session goes into configuration mode, and does a commit for some configuration when a prior SSH session configuration commit was still in process, a deadlock situation may occur.
GEN7-30715	Unnecessary `tHaImPrefTask` stack traces were being printed in with a High Availability pair when both WAN Load Balancing and IPv6 are enabled.
GEN7-31151	A Site to Site VPN phase 2 tunnel with the IKE version configured as IKEv1 Main Mode does not display any VPN tunnel statistics.
GEN7-31889	Stack-based buffer overflow in SonicOS potentially resulting in Denial-of-Service (DoS).
GEN7-31890	Potential exposure of sensitive information to an unauthorized user via SNMP.
GEN7-31990	Potential exposure of Wireless Access Point (WAP) sensitive information via SNMP.
GEN7-31991	Improper restriction of TCP communication channel potentially resulting in Denial-of-Service (DoS).
GEN7-31992	Allocation of resources without limits or throttling can potentially result in HTTP DoS via the Content Filtering Service (CFS).
GEN7-31994	Unnecessary `tNetObjMgr` stack traces are displayed on the console.

Issue ID	Issue Description
GEN7-32418	The OpenSSL library can enter an infinite loop when parsing an invalid certificate, potentially resulting in Denial-of-Service (DoS).

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-31993, GEN7-31288, GEN7-30711, GEN7-30707, GEN7-30540, GEN7-30539, GEN7-30537, GEN7-30042, GEN7-29767, GEN7-29652, GEN7-29585, GEN7-29386, GEN7-29340, GEN7-29290, GEN7-27287, GEN7-26996

Known Issues

Issue ID	Issue Description
GEN7-29535	The console prints a `tTimerTask` stacktrace about every hour. There is no functional effect.
GEN7-31879	Configuration changes on the **Decryption** policy page are not listed in the log files and cannot be audited.
GEN7-31899	Configuration changes on the **DoS** policy page are not listed in the log files and cannot be audited.
GEN7-31900	Configuration changes on the **DoS Action Profile** page are not listed in the log files and cannot be audited.
GEN7-32261	OSPFv3/RIPng cannot be established over a trunked VLAN or sub-VLAN interfaces.
GEN7-32540	A crash may be seen with a stacktrace for `DP-engine-0` in a High Availability Pair causing failover when running a heavy load of mixed traffic, UDP traffic, and OSPF routes when DPI-SSL Decryption Policies and Bandwidth Management are configured.
GEN7-32620	A crash may be seen with a stacktrace for `delayedLog.c` in a High Availability Pair causing failover when running a heavy load of mixed traffic, UDP traffic, and OSPF routes when DPI-SSL Decrytion Policies and Bandwidth Management are configured.

Version 7.0.1-5052 April 2022

April 2022

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5052
NSa Series	7.0.1-5052
NSv Series	7.0.1-5052
NSsp Series	7.0.1-5052

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 5700
- NSa 6700
- NSsp 10700
- NSsp 11700
- NSsp 13700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

SonicOS NSv deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-31534	*NSv series only:* Improper restriction of TCP communication channel potentially resulting in DoS
GEN7-31742	*NSv series only:* Potential exposure of sensitive information to an unauthorized user via SNMP
GEN7-31870	*NSa series, NSsp series, TZ series:* Potential exposure of Wireless Access Point (WAP) sensitive information via SNMP
GEN7-31996	*NSv series only:* Allocation of resources without limits or throttling can potentially result in HTTP DoS via the Content Filtering Service (CFS)
GEN7-31997	*NSa series, NSsp series, TZ series:* Stack-based buffer overflow in SonicOS potentially resulting in DoS
GEN7-30684	Offline registration on KVM using a manual keyset fails.
GEN7-30532	Core 0 gradually increases to 100% utilization after about 12 hours.
GEN7-30420	High Availability with Stateful Failover-enabled connections may not be fully being synchronized between active and standby units.

Issue ID	Issue Description
GEN7-30388	High Availability units may stop responding and fail over to Secondary, reporting a DP crash.
GEN7-30385	After importing Settings migrated from an NSa 3600 to an NSa 3700, navigating to the NAT page displays the error: `An error has occurred but the cause could not be determined at this time`.
GEN7-30375	A crash may be observed in configuration auditing timer when the device is rebooted.
GEN7-30022	The **Search** field in the **ARP** table only allows for the entry of one character.
GEN7-29639	When a Bridge member is bound bind to a WAN interface and firewalling is enabled, the firewall cannot be accessed when the system pings the WAN subnet. All traffic, including LAN to WAN, is also affected
GEN7-29637	Incorrect values for memory usage may be reported when using SNMP.
GEN7-29383	Firewall appliances may stop responding.
GEN7-29246	High Availability timeout customization changes to help with large configuration files synchronization between Active and Idle units have been improved.
GEN7-29150	Default Service Objects for ICMPv6 are missing in the web management interface.
GEN7-29051	In a Stateful Failover configuration, the active firewall may be unable to send cache remove packets to an idle firewall, reporting `No buffer`, causing connection cache to increase rapidly on the idle firewall.
GEN7-29048	A firewall may drop valid traffic as `IP spoof dropped` over point-to-point connections with probing enabled on a policy-based route.
GEN7-29043	Client DPI-SSL may cause high CPU utilization.
GEN7-29007	Changing the maximum transmission unit (MTU) of a Virtual interface fails without displaying an error.
GEN7-28979	The **Exclusion Group** setting on **App Control** changes to **None** when the device is restarted.
GEN7-28950	**Packet Monitor** displays more packets than are selected in the **Filter**.
GEN7-28911	Anti-Spam does not accept `.local` hostname under a LDAP server configuration of CASS. It fails with the error `host name is empty or not valid`.
GEN7-28861	Transparent range host and range objects are not available in the **Transparent Range** drop-down list on the transparent interface configuration page when the primary WAN is set to any value other than **X1**.
GEN7-28848	A device registered offline with the signatures updated will not allow the creation of an Application Group.
GEN7-28847	Border Gateway Protocol (BGP)-related access rules that were deleted are added again after when the device is restarted. An option on the Diagnostics page, **Disable auto-added BGP access rules** was added to resolve this issue. When checked, this option will remove any existing automatically-added BGP rules and prevent the automatically-added BGP rules from being added again in the future.

Issue ID	Issue Description
GEN7-28793	Modifying third-party SSO API client settings displays the error: `Host name / IP address: The host name/IP address must be unique`.
GEN7-28782	A firewall appliance may stop responding intermittently.
GEN7-28762	Some EICAR test files do not get blocked by Gateway Anti-Virus.
GEN7-28744	Unable to create a cloud backup with the error `Cloud backup service is unavailable`.
GEN7-28682	System logs file cannot be downloaded from the Secondary Storage. When the button to download the file is clicked, no popup window is displayed by the browser to save the file.
GEN7-28622	When editing a multi-path route using unnumbered tunnel interfaces as the next hop interfaces, the error is displayed: `interfacex value is unreasonable`.
GEN7-28535	The error `Enter a valid IPV4 addresss for default target in X1` is displayed when trying to change Load Balancing and Failover Group settings so the order of interfaces is different for basic failover.
GEN7-28495	SSL-VPN Services group is inheriting all VPN Access objects from its member users,
GEN7-28464	Unable to add or edit an WLAN interface when **Only allow traffic generated by a SonicPoint/SonicWave** is disabled. Attempting to causes this error to be displayed: `Command 'no auto-discovery' does not match`.
GEN7-28447	Communication between two subnets is not blocked by the Security policy when using secondary subnets on the same interface.
GEN7-28412	E-mails on the mail server are sometimes not deleted and the connection to the mail server is not disconnected even if password-protected ZIP attachment files are detected as having a virus by Gateway Anti-Virus. This occurs with **Gateway Anti-Virus**, **POP3 protocol Inbound Inspection**, and **Restrict Transfer of password-protected ZIP files** settings enabled.
GEN7-28406	When clicking the next arrow to items in the **IP address** column on the **On Check Network Settings** page of **Diagnostics** does not redirect to the setting spage for the specific server.
GEN7-28397	Link Aggregation Control Protocol (LACP) on 40GB Interfaces (X33) fails after rebooting NSa 6700 devices.
GEN7-28388	Unable to configure the fiber interfaces on the **Portshield Port Graphics** page, displaying the error `Command 'link-speed auto-negotiate' does not match`.
GEN7-28384	Unable to configure the interface in Portshield to WLAN zone
GEN7-28360	When Failover and Load Balancing is disabled, failover does not occur when shutting down the primary WAN.
GEN7-28307	The error `Unknown Reason` is displayed when configuring **Local Users & Groups Settings** page in **Non-Config** mode,

Issue ID	Issue Description
GEN7-28269	Deploying an NSv virtual device to an existing Virtual Network in Azure using Marketplace or Templates results in the network secrity group not being associated with the X1 WAN Subnet.
GEN7-28176	The **Guest Services** configuration for **Session Synchronization** displays incorrect values in the web management interface and command-line interface (CLI).
GEN7-28148	\`GroupList\` (DH) failed to generate after rebooting causing VPN to not come up.
GEN7-28144	Unable to export console logs via FTP using the command-line interface (CLI).
GEN7-28123	Data Plane Core utilization reaches 100% intermittently, causing the web management interface to lag and disrupting internet access to network hosts
GEN7-28038	Possible buffer overflow that can be caused by an invalid parameter used by communication protocols between firewall and backend.
GEN7-27950	Unable to manually add the parent switch to a High Availability pair, with this error: `Index of the Extended Switch instance`.
GEN7-27592	The SSL-VPN RDP HTML5 Bookmark disconnects intermittently while resizing the window or itself without any changes.
GEN7-26764	The **Edit Lists** selection box for **Authentication Partition** always shows `Available Radius servers` even of other types are chosen such, as SSO agents or LDAP servers.
GEN7-26758	**Transparent range** displays address objects and address groups that are not part of WAN subnet.
GEN7-26447	When primary storage option is chosen for log storage, the file location for log files is not updated. The file location still shows `extended`.
GEN7-26136	While connected using NetExtender, users may be frequently disconnected while trying to move, copy, open, or upload files to a shared drive.
GEN7-26089	When 100M/10M speeds are forced on an interface, shutting down the interface and bringing it back by clicking the **Enabled** toggle button results in a `No link` error.
GEN7-26063	The Auto-negotiation of multiple speeds does not work on the QSFP+ (40G) and QSP28 (100G) ports,
GEN7-24957	An error is displayed with an undetermined cause the first time users log in using Two-Factor Authentication.
GEN7-24835	Address Objects bound to a custom Public zone as well as Trusted zone are not displayed in the **Transparent Range** list while configuring an interface in Transparent Mode.
GEN7-24821	Content Filtering policies block the web pages as expected, but firewall log events are not reporting any block messages and Analytics reporting shows that access to the website is allowed.
GEN7-24658	Blade synchronization issues may be seen when trying to log in using the default administrator credentials when using Two-Factor Authentication.

Issue ID	Issue Description
GEN7-20540	The **Route Policy Details** for the source and destination routes are incorrect on the **IPv6 Connections** page on the backup unit of a High Availability pair.
GEN7-20422	A Guest user having Group membership as "Guest Administrators" gets an error when logging in and is unable to use "Auto-generate password" feature for guest accounts according to assigned guest profile, is unable to export guest user list, and, when using the print icon, the password is not displayed on the paper.
GEN7-15543	On NSsp 15700 appliances, a BGP/OSPF neighbor cannot be established on a numbered VPN tunnel interface when the VPN policy is established on a non-master blade.
GEN7-13640	Packet Monitor configuration is synchronized across a High Availability pair instead of being prevented.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-22240, GEN7-23631, GEN7-23834, GEN7-24321, GEN7-25750, GEN7-25751, GEN7-25813, GEN7-26604, GEN7-26622, GEN7-26793, GEN7-27090, GEN7-27367, GEN7-27471, GEN7-27508, GEN7-27512, GEN7-27542, GEN7-27555, GEN7-27725, GEN7-27727, GEN7-27728, GEN7-27863, GEN7-27866, GEN7-27927, GEN7-27948, GEN7-27954, GEN7-27957, GEN7-27958, GEN7-28005, GEN7-28022, GEN7-28055, GEN7-28056, GEN7-28082, GEN7-28084, GEN7-28111, GEN7-28116, GEN7-28120, GEN7-28124, GEN7-28155, GEN7-28163, GEN7-28175, GEN7-28177, GEN7-28182, GEN7-28222, GEN7-28223, GEN7-28272, GEN7-28276, GEN7-28278, GEN7-28366, GEN7-28386, GEN7-28391, GEN7-28403, GEN7-28413, GEN7-28436, GEN7-28444, GEN7-28462, GEN7-28480, GEN7-28492, GEN7-28496, GEN7-28497, GEN7-28508, GEN7-28547, GEN7-28548, GEN7-28570, GEN7-28595, GEN7-28596, GEN7-28617, GEN7-28624, GEN7-28626, GEN7-28657, GEN7-28665, GEN7-28692, GEN7-28717, GEN7-28735, GEN7-28740, GEN7-28741, GEN7-28745, GEN7-28747, GEN7-28748, GEN7-28753, GEN7-28754, GEN7-28769, GEN7-28778, GEN7-28779, GEN7-28799, GEN7-28829, GEN7-28830, GEN7-28856, GEN7-28857, GEN7-28862, GEN7-28872, GEN7-28889, GEN7-28901, GEN7-28914, GEN7-28934, GEN7-28978, GEN7-29084, GEN7-29103, GEN7-29111, GEN7-29165, GEN7-29174, GEN7-29176, GEN7-29184, GEN7-29237, GEN7-29247, GEN7-29264, GEN7-29288, GEN7-29298, GEN7-29318, GEN7-29339, GEN7-29344, GEN7-29350, GEN7-29355, GEN7-29543, GEN7-29548, GEN7-29619, GEN7-29683, GEN7-29740, GEN7-29768, GEN7-29772, GEN7-29773, GEN7-29796, GEN7-29809, GEN7-29830, GEN7-29843, GEN7-29844, GEN7-30018, GEN7-30083, GEN7-30308, GEN7-30333, GEN7-30445, GEN7-30448, GEN7-30482, GEN7-30505, GEN7-30532, GEN7-30595, GEN7-30619, GEN7-30741, GEN7-30768, GEN7-30772, GEN7-30908, GEN7-30990, GEN7-31089

Known Issues

Issue ID	Issue Description
GEN7-31453	Custom static routes are not automatically disabled when a WAN probe fails and goes into failover.

Issue ID	Issue Description
GEN7-31247	Native Bridge Mode Pair causes IP traffic drops from and between the paired VLAN interfaces and causes the firewall web management interface to become inaccessible.
GEN7-30899	In networks with ISPs that have high packet loss, DPI-SSL may consume additional memory for each decrypted connection.
GEN7-30810	Naming a Service group as a number prevents service objects from using that number as a port.
GEN7-30418	Not able to change the **Default target IP** under **WAN failover and Load balancing Probe settings** if using `0.0.0.0`.
GEN7-29872	The error message `The server is not sending intermediate certificate` may be displayed when using **Server DPI-SSL**.
GEN7-29867	Trying to add an **All Deny** access rule from **WAN > WAN** generates the error `Rule Blocks Management Rule(s).`
GEN7-29853	Settings are not saved when importing LDAP users and assigning the user quota on the **Import** page. **Workaround:** Assigning per user will save the setting.
GEN7-29640	When importing settings using the Migration Tool, Switch settings are not imported.
GEN7-29552	Unbinding the Time-based one-time password (TOTP) key from the **User Login Status** page did not work if the user password does not meet the complexity constraints.
GEN7-29535	The console displays a `tTimerTask` stacktrace about every hour.
GEN7-29415	The VLAN subinterface does not show correct maximum transmission unit (MTU) in the web management interface when Jumbo frames are enabled.
GEN7-29262	Traffic failed to pass through VPN tunnel interface for the tunnel VPN policy established on non-master blades when VPN is bound to a VLAN interface and the VLAN's parent interface is unassigned. **Workaround:** Assign the parent physical interface for the VLAN.
GEN7-29210	Unable to add 10 GB SFP+ interfaces for Port Mirroring.
GEN7-29058	A wildcard FQDN object will not resolve subdomains unless a *www* FQDN object is also created.
GEN7-28816	Cannot ping from VLAN interface trunked with custom VLAN ID after rebooting the unit.
GEN7-28760	Multi-Instance virtual firewalls with a 100GbE port attached displays the interface as having a 1GbE link.
GEN7-28475	The web management interface reports `Command` *`xxx`* `did not match` when the guest service is enabled on the LAN zone and the same IP address is used by an administrator and guest to manage the web management interface.
GEN7-26488	Native Bridge Mode Pair causes IP traffic drops from and between the paired VLAN interfaces and causes the firewall web management interface to become inaccessible.

Issue ID	Issue Description
GEN7-24141	New devices may not be acquired by Network Security Manager that have settings for VoIP are imported from an older (pre-2020) device.
GEN7-19015	Cannot connect to Layer Two Tunneling Protocol (L2TP) with packets dropped as the packet does not match traffic selectors if the L2TP clients are behind a network address translation (NAT) IP address assignment.

Version 7.0.1-5030 December/October 2021

October 2021

This version of SonicOS7.0.1 (7.0.1-5030-R780) is a maintenance release for currently shipping NSsp 15700 platform and resolves issues found in previous releases.

Supported Platforms

The platform-specific versions for this release apply to NSsp 15700 platforms.

Resolved Issues

Issue ID	Issue Description
GEN7-30375	A crash was observed during reboot in the configuration auditing timer.
GEN7-30332	A crash was observed when accessing the IPv6 address cache with a mix of IPv4 and IPv6 users being repeatedly logged in and out.
GEN7-30022	The Search in the ARP table only allows a 1 character entry.
GEN7-30021	Incorrect IPv6 addresses are displayed for logged in users on the **User Status** page.
GEN7-29792	Loading settings with several IPv6 VLANs configured causes devices configured in High Availability to continuously failover and failback.
GEN7-29623	In L3 Port Aggregation, the Aggregate Port does not show the correct link state on the Dashboard page of the user interface.
GEN7-29620	Changing verification security level on the SSO 3rd Party API Configuration Advanced page on the interface triggers an error message: **Host name/IP Address: the host name/IP address must be unique**.
GEN7-29593	A memory leak from the SSO API was observed when returning multiple errors in response to an SSO API request with multiple users.
GEN7-29592	Blade mismatch warnings are being seen for SSO API user authentication with large number of users.
GEN7-29590	An intermittent crash is seen when adding SSO users via 3rd party API and IPv6 and IPv4 groups overlap while IPv4/IPv6 traffic is present.
GEN7-29415	VLAN subinterface does not show correct MTU in the user interface when jumbo frames are enabled.
GEN7-29412	When accessing the Dashboard the first time, the Front Panel widget does not show the interface status indicators.

Issue ID	Issue Description
GEN7-29246	HA timeout customization changes were improved to help large configuration files synchronize between Active and Idle units.
GEN7-29150	Default Service Objects for ICMPv6 are missing in user interface.
GEN7-28793	Modifying 3rd party SSO API client settings results in error: **Host name / IP address: The host name/IP address must be unique**.
GEN7-28338	A number of IPv6 SSO inefficiencies in the mechanism for inter-blade user sync requests were fixed (those which request other blades to send something back and then wait for it).
GEN7-20540	Route Policy Details for source and destination routes are wrong on IPv6 connections page on the backup unit of a High Availability pair.

Known Issues

Issue ID	Issue Description
GEN7-30590	Importing settings fail and trigger a trace indicating a post file HTTP issue through the API.
GEN7-30560	In response to a user accessing the WAN from LAN using a security rule containing the group Everyone, the device shows an undetermined error when trying to change the password after login.
GEN7-30559	A reboot is seen during LDAP import of a large number of users.
GEN7-30459	On the LDAP User Import page, for the user groups that were read form the LDAP Server, only the first LDAP Group location shows any users.
GEN7-30065	When trying to manually log out users from the interface, once they're populated and active, produces an error: **command 'killuser ...' does not match**.
GEN7-30009	Security Policies page shows **No Data** momentarily when loading over 600 entries.
GEN7-29777	The user interface is very slow when refreshing the User Group page with over 2800 user groups in it.

October 2021

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5030
NSa Series	7.0.1-5030
NSv Series	7.0.1-5030
NSsp Series	7.0.1-5030

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 6700
- NSsp 13700
- NSsp 15700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

SonicOS NSv deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-25465	Cannot delete LDAP user group
GEN7-25712	Compatibility issue with certain switch vendor 25G implementations
GEN7-26035	OSPF becomes disabled on the unnumbered VPN Tunnel Interface after adding LAG's member when it's bound to a L2 LAG port
GEN7-26419	*NSsp 15700 only:* The Interface Link Speed is not configurable on the web management interface, but is configurable on the command-line interface (CLI)
GEN7-26507	Delay in call setup of 10-60 seconds may be experienced when a SIP call is made.
GEN7-26613	Putting a serial number using lower case characters in the Serial Number field on the **High Availability > Settings** page for a Secondary Firewall is not allowed.
GEN7-26653	The management console for Capture Client URI "`captureclient-36.sonicwall.com` has not been added to the allowed list, which will cause Capture Client to be unable to be installed and licensed, making its policy and certificate unavailable.
GEN7-26710	Administrators are unable to change partition for a newly added policy on the **Device > Users > Authentication Partition** page.
GEN7-26785	If devices have Capture Client installed, Endpoint Enforcement does not allow access to the devices.
GEN7-26827	The 10G RJ45 interface (X16-X19) Link Speed displays auto-negotiated to 5Gbps on the **Interfaces** page

Issue ID	Issue Description
GEN7-27038	On the **Device > Users> LDAP configuration** page, the child LDAP server are not shown in the web management interface.
GEN7-27047	When using High Availability, the Certificate for Administration is not used on the Secondary Appliance after initial synchronization.
GEN7-27429	*NSA 6700 only:* Cannot create LACP on 40GB Interfaces (X33)
GEN7-27441	Guest Services user interface authorization fails on a Guest Services-enabled LAN zone.
GEN7-27514	The Event Logs is not showing any events for OSPF.
GEN7-27823	Configuring **Ratio** mode for an LB group fails with an error message: `Command 'rank 1' does not match`.
GEN7-27936	The network security appliance may become nonfunctional when switching between main power and battery backup (UPS).
GEN7-27976	When using a Dell switch in a Daisy-chain configuration Portshielding does not work on the parent switch.
GEN7-28110	Network security appliances that have settings migrated from a previous generation appliance fails during Network Security Manager acquisition.
GEN7-28225	Unable to restore settings from a cloud backup.
GEN7-28270	Clicking **Cancel** on when confirming whether to reset to factory defaults still causes the appliance to reset to the factory defaults.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-28157, GEN7-27978, GEN7-27955, GEN7-27950, GEN7-27930, GEN7-27834, GEN7-27766, GEN7-27747, GEN7-27712, GEN7-27703, GEN7-27671, GEN7-27670, GEN7-27571, GEN7-27515, GEN7-27473, GEN7-27453, GEN7-27432, GEN7-27239, GEN7-27216, GEN7-27203, GEN7-27181, GEN7-27174, GEN7-27138, GEN7-27095, GEN7-27094, GEN7-27062, GEN7-27041, GEN7-27025, GEN7-26853, GEN7-26819, GEN7-26773, GEN7-26716, GEN7-26715, GEN7-26551, GEN7-26518, GEN7-26346, GEN7-25966, GEN7-24904, GEN7-24809, GEN7-23834

Known Issues

Issue ID	Issue Description
GEN7-28144	Unable to export console logs using FTP from the console. **Workaround:** Use SCP to transfer files.

Issue ID	Issue Description
GEN7-28238	In WAN Load Balancing and Failover setup, traffic flows from the backup WAN even when the Primary is at the Rank 1 and active after a cold boot or a firmware upgrade. **Workaround:** Swap the rank on the Load Balancing settings and then swap back to the original configurations.
GEN7-28269	Deploying NSv on Azure to an existing VNET does not associate NSG to the X1 WAN subnet. **Workaround:** Manually configure NSG on the existing WAN subnet or on the NSv X1 interface.
GEN7-28360	With Failover and Load Balancing disabled failover does not occur when shutting down primary WAN.
GEN7-28384	Unable to configure the interface in Portshield to a WLAN zone.
GEN7-28388	Trying to configure the fiber interfaces on the **Portshield Port Graphics** page causes the error `Command 'link-speed auto-negotiate' does not match` to be displayed.
GEN7-28397	*NSa 6700 only:*LACP on 40GB Interfaces (X33) fails after rebooting the appliance.
GEN7-28463	WLB Type Spillover is working with interfaces in reverse of how it is configured.

Version 7.0.1-5026 September 2021

September 2021

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Supported Platforms

ⓘ **IMPORTANT:** Only these SonicWall network security appliances are supported by this release of SonicOS 7.0.1:

Platform	Firmware Version
NSa 6700	7.0.1-5026

Resolved Issues

Issue ID	Issue Description
GEN7-26344	The network security appliance receives a signal to abort during restart, causing network interfaces to fail to establish links.
GEN7-27399	The web management interface for a network security appliance becomes unavailable when using the X0 port.

Version 7.0.1-5023 August 2021

August 2021

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Supported Platforms

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5023
NSa Series	7.0.1-5023
NSv Series	7.0.1-5023
NSsp Series	7.0.1-5023

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 6700
- NSsp 13700
- NSsp 15700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

NSv 270/470/870 deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-24501	When **Physical Monitoring only** is enabled, the VLAN interface set as the primary WAN interface cannot failover after its parent interface is shut down.
GEN7-25650	OSPF routes not showing as Active.
GEN7-26235	Some changes on the **Failover & LB** pages cause unwanted reordering of **LB Group** values in the web management interface .
GEN7-26534	For WAN interfaces, the settings cannot be changed between **Logical/Probe Monitoring enabled** and **Physical Monitoring only**.
GEN7-26645	Changes to the **User Authentication Method** are not being saved when selected under **User Settings**.
GEN7-26741	Cannot delete unwanted address groups.
GEN7-26987	After setting the **VLAN ID** to 3 (on the **NETWORK > Firewall > Advanced > Internal VLAN** page), DHCP requests are answered from X1 instead of X0, preventing access to the web management interface.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-27591, GEN7-27543, GEN7-27007, GEN7-26908, GEN7-26624, GEN7-26571, GEN7-26338, GEN7-26179, GEN7-23551

Known Issues

Issue ID	Issue Description
GEN7-26785	If devices have Capture Client installed, Endpoint Enforcement does not allow access to the devices.
GEN7-27823	Configuring **Ratio** mode for an LB group fails with an error message: `Command 'rank 1' does not match`. **Workaround:** Use the command-line interface (CLI) to configure or change to ratio-based mode.
GEN7-27849	An error is displayed when Group Always On is selected as the Exclusion Address for an App Control Policy type.

Version 7.0.1-5019 August 2021

August 2021

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves issues found in previous releases.

Supported Platforms

ⓘ **IMPORTANT:** Only these SonicWall network security appliances are supported by this release of SonicOS 7.0.1:

Platform	Firmware Version
NSa 4700	7.0.1-5019
NSa 6700	7.0.1-5019
NSsp 13700	7.0.1-5019

Resolved Issues

Issue ID	Issue Description
GEN7-26374	High Availability is not working correctly on 10GB interfaces. The interface indicates that it is not connected.
GEN7-26816	**LAN Bypass** is not set **Off** by default.
GEN7-26990	Resetting the power while in Safe Mode during a **Wipe** process will put the network security appliance in an unrecoverable state.

Known Issues

Issue ID	Issue Description
GEN7-27207	After enabling **Override Speed**, the **Link Speed** field is unavailable and cannot be set.

Version 7.0.1 July 2021

July 2021

This version of SonicOS 7.0.1 is a maintenance release for existing platforms and resolves many issues found in previous releases. This release also introduces support for the SonicWall NSa 4700, NSa 6700 and NSsp 13700 network security appliances.

Supported Platforms

ⓘ | **NOTE:** Starting in this release, SonicWall has dropped the 'R' label from SonicOS release numbers.

The platform-specific versions for this unified release are all the same:

Platform	Firmware Version
TZ Series	7.0.1-5018
NSa Series	7.0.1-5018
NSv Series	7.0.1-5018
NSsp Series	7.0.1-5018

The following SonicWall network security appliances are supported by this release of SonicOS 7.0.1:

- NSa 2700
- NSa 3700
- NSa 4700
- NSa 6700
- NSsp 13700
- NSsp 15700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

NSv 270/470/870 deployments are supported on the following platforms:

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

Resolved Issues

Issue ID	Issue Description
GEN7-15543	On NSsp 15700, BGP/OSPF failed to establish on a numbered VPN tunnel interface when VPN policy is established on a non-master blade.
GEN7-16351	When adding or editing an LDAP server on an NSsp 15700 with Authentication Partitioning enabled, there is no Partition field or option.
GEN7-21526	After being disconnected, a second PPPoE connection does not connect until the firewall is rebooted.
GEN7-21977	Adding, deleting, configuring or managing a Dell X-Series switch on an NSa 3700 does not work as expected and displays the error, "Error: Index of the Extended Switch Instance."
GEN7-22545	Packet drops on WAN interface cause interruption in internet access.
GEN7-22706	Detecting a SonicWall Switch beyond the first level in multi-level daisy chaining takes a long time.
GEN7-22772	VLANs of the parent SonicWall Switch are not configured properly when using multi-level chaining.
GEN7-22826	RDP service bookmark cannot be launched from the portal page in Internet Explorer and Safari browsers.
GEN7-22868	LDAP user and user group import should not show users/groups that were previously imported.
GEN7-22950	When updating signatures manually, the Signature File ID is incorrectly displayed as '3' in the POLICY | Security Services > Summary page. It should be '6'.
GEN7-22972	A LAN PC cannot open an SSH Terminal session after disabling and then enabling SSH management on the X0 interface.
GEN7-23108	The X1 interface cannot be enabled administratively after an NSv is registered using the manual keyset.
GEN7-23121	After upgrading tenants to new firmware, the tenants end up in failed state after 1 to 2 hours.
GEN7-23168	Serial Number and Auth Code should not be required when logging into the MySonicWall account after Manual Key Registration.
GEN7-23211	On NSv, the Protocol page is missing in the WAN PPPoE interface edit window.
GEN7-23389	DMZ Address Groups does not appear in the drop-down list on the firewall while configuring the interface in Transparent Mode.
GEN7-23408	Anti-Spyware signatures are not enabled by globally enabling Prevent/Detect.
GEN7-23410	When navigating to the Network > Zones page in the Classic user interface of a firewall running SonicOS 7.0.1, the user is redirected to the login page.

Issue ID	Issue Description
GEN7-23481	When the portshield host port has no link, the PortShield Mode management traffic does not work on any other linked portshield member ports.
GEN7-23502	There are issues with enabling and disabling interfaces.
GEN7-23504	Change the default algorithm to AESGCM-256 for non GroupVPN policies.
GEN7-23526	SSL VPN Virtual office RDP HTML5 bookmark does not work as expected.
GEN7-23583	On NSsp 15700, there is a Security policy issue when using both Content Filter Service (CFS) and user level authentication.
GEN7-23793	Additional gateways are not populated in a Multi-Path Route policy.
GEN7-23848	The Match Object field is not populated when creating or editing a custom match.
GEN7-23911	Route policies do not show correct address objects while trying to edit them.
GEN7-23957	Portshielding a Switch interface (Switch 2) to a VLAN interface on uplink results in an error.
GEN7-24136	Double interfaces are shown in the interface selection list during backend server communication.
GEN7-24137	During backend server communication, selection of a specific interface does not work as expected, but always appears as ANY.
GEN7-24224	Valid TCP packets with Urgent data are dropped.
GEN7-24458	On NSv for AWS, APIs do not show custom tags and values.
GEN7-24521	On NSv for AWS, AWS VPN does not show VPC details.
GEN7-24533	Login fails with auto generated guest accounts and the error, "Module not ready" is reported.
GEN7-24577	TCP Urgent - UI Implementation
GEN7-24741	In DNS settings after selecting the Specify DNS Servers Manually option and clicking Accept, the selected option is changed to Inherit DNS Settings Dynamically from WAN Zone.
GEN7-25457	On multi-blade NSsp, an error is displayed when enable/disable RIP/OSPF for a numbered tunnel interface.
GEN7-25770	Adding a multi-path route policy failed when configuring a VPN tunnel interface as a non-first interface.

Issue ID	Issue Description
GEN7-25830	The Use Address Object drop-down menu does not display the Address Object created by the user in the GATEWAY AV EXCLUSION LIST.
GEN7-26006	Resolved a PCI Compliance failed issue with error "HTTP Security Header Not Detected" on SSL-VPN portal.
GEN7-26336	With Virtual MAC addressing enabled, the firewall sends a Gratuitous ARP reply using the default MAC address after the interface renews its DHCP lease, resulting in the connection being lost.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-18760, GEN7-20414, GEN7-21047, GEN7-21094, GEN7-21234, GEN7-21357, GEN7-22055, GEN7-22353, GEN7-22362, GEN7-22480, GEN7-22545, GEN7-22684, GEN7-22685, GEN7-22826, GEN7-22877, GEN7-23173, GEN7-23184, GEN7-23191, GEN7-23220, GEN7-23281, GEN7-23287, GEN7-23329, GEN7-23363, GEN7-23364, GEN7-23368, GEN7-23375, GEN7-23389, GEN7-23392, GEN7-23411, GEN7-23453, GEN7-23490, GEN7-23518, GEN7-23526, GEN7-23531, GEN7-23541, GEN7-23549, GEN7-23565, GEN7-23572, GEN7-23582, GEN7-23700, GEN7-23760, GEN7-23798, GEN7-23807, GEN7-23840, GEN7-23870, GEN7-23871, GEN7-23873, GEN7-23885, GEN7-23904, GEN7-23911, GEN7-23935, GEN7-23939, GEN7-23966, GEN7-23987, GEN7-23991, GEN7-23992, GEN7-24034, GEN7-24054, GEN7-24056, GEN7-24057, GEN7-24059, GEN7-24060, GEN7-24061, GEN7-24062, GEN7-24063, GEN7-24064, GEN7-24109, GEN7-24134, GEN7-24135, GEN7-24140, GEN7-24178, GEN7-24187, GEN7-24292, GEN7-24305, GEN7-24329, GEN7-24348, GEN7-24429, GEN7-24567, GEN7-24568, GEN7-24587, GEN7-24633, GEN7-24689, GEN7-24693, GEN7-24751, GEN7-24756, GEN7-24810, GEN7-24819, GEN7-24847, GEN7-24884, GEN7-24888, GEN7-24895, GEN7-24933, GEN7-24971, GEN7-24994, GEN7-25000, GEN7-25456, GEN7-25473, GEN7-25521, GEN7-25538, GEN7-25566, GEN7-25568, GEN7-25606, GEN7-25624, GEN7-25746, GEN7-25818, GEN7-25819, GEN7-25833, GEN7-25944, GEN7-26348

Known Issues

Issue ID	Issue Description
GEN7-22389	On NSsp 15700, the State Sync function displays a critical unexpected error that the Retransmit buffer's sequence number does not match the array element.
GEN7-23716	When a user logs in with the admin credentials or with user credentials that have SonicOS administrator privileges and then navigates to the Network > Zones page, the user is logged out and redirected to the login page.
GEN7-24864	Local packet mirror does not take effect.
GEN7-24957	On NSsp 15700, an error is always displayed the first time a user logs in with Time-based One Time Password (TOTP) enabled.
GEN7-25016	External storage display is wrong in TSR and in the SonicOS web management interface.

Issue ID	Issue Description
GEN7-25712	25G Direct Attach Cables (DAC) might not auto-negotiate speed and/or error correction on the NSsp 13700 X24-X31 ports.
GEN7-26035	OSPF becomes disabled on the unnumbered VPN tunnel interface after adding the link aggregation LAG's member when it is bound to a Layer 2 LAG port.
GEN7-26063	Auto-negotiation of multiple speeds might not work on the SFP/QSFP ports on NSsp 13700. **Workaround**: Manually specify the link speed.
GEN7-26089	100M/10M interface status shows "No link" after shutdown/no shutdown by toggling the Enabled button. **Workaround**:Set Link Speed to Auto Negotiate or 1 Gbps Duplex.
GEN7-26093	SSL VPN will not work if DPI and Stateful Firewall Security is applied before enabling SSL VPN.
GEN7-26154	PortShield is enabled by default when High Availability is enabled in Internal Settings.
GEN7-26188	The LED for LAN bypass does not work as expected.
GEN7-26204	VPN policy does not show gateway and networks if quotes are used in the VPN name.
GEN7-26374	High Availability on 10G interfaces sometimes shows a connected interface as not connected.
GEN7-26419	On NSsp 15700, interface Link Speed is not configurable in the SonicOSX web management interface, but is configurable in the CLI.
GEN7-26444	Log files stored in External Storage cannot be deleted when using the SonicOS web management interface.
GEN7-26447	File location is not correct when Primary Storage is chosen for log storage.
GEN7-26465	Included or Excluded Users/Groups settings of IPS Signature cannot be imported.
GEN7-26474	Unable to set WAN IP manually on SonicOS Setup Guide page when using Firefox browser.
GEN7-26534	Cannot change the logical probe settings to Physical monitoring and vice versa for WAN interfaces.
GEN7-26645	On NSa 4700, NSa 6700 and NSsp 13700, changes are not saved in user authentication method drop-down field under user settings.
GEN7-26710	On NSa 4700, NSa 6700 and NSsp 13700, not able to change partition in DEVICE | Users > Authentication Partition page for a newly added policy.
GEN7-26726	Purge option to delete log files from storage cannot be selected if two or more files are selected.
GEN7-26827	On NSsp 13700, the 10G RJ45 interface (X16-X19) Link Speed auto-negotiates to 5 Gbps when the cable is more than 10 feet long.
GEN7-26871	TSR does not show files present on the two storage devices.

Issue ID	Issue Description
GEN7-26888	SonicOS web management certificate did not have CN content of Subject and Issuer after changing Certificate Selection settings.
GEN7-26987	DHCP leases offered from X1 (WAN) are in the IP address range from the X0 lease scope. Occurs when the internal reserved VLAN is changed from the SonicOS/X 7.0.1 default by a converted or imported SonicOS 6.5 configuration. **Workaround**: Configure reserved VLAN as the SonicOS/X 7.0.1 default of 3968 or higher as the starting VLAN.
GEN7-27038	On NSa 4700/6700 or NSsp 13700, child LDAP servers are not shown in LDAP server list in the contemporary user interface. **Workaround**: Configure the LDAP servers using the classic user interface.

Version 7.0.1 June 2021

June 2021

This release resolves a number of critical issues and other issues found in previous releases.

The platform-specific versions for this release are:

Platform	Firmware Version
TZ Series	7.0.1- R1456
NSa Series	7.0.1- R1456
NSv Series	7.0.1-R1282 / 7.0.1-R1283
NSsp Series	7.0.1-R579

Important

If you are running any previous versions of SonicOS 7.0.1, SonicWall recommends upgrading to this release.

Resolved Issues

Issue ID	Issue Description
GEN7-23005	Configuring the WAN interfaces in PPPoE mode makes all the interfaces vanish from the page.
GEN7-23108	X1 cannot be enabled administratively after an NSv is registered using the manual keyset.

Issue ID	Issue Description
GEN7-23121	After upgrading tenants to a newer firmware version, the tenants quickly (1 - 2 hours) end up a failed state.
GEN7-23389	The selection for DMZ Address Groups does not show up in the drop down list on the firewall while configuring the interface in Transparent Mode.
GEN7-23481	When the X0 port is disconnected, the PortShield mode management traffic does not work correctly on any spare interface on TZ platforms.
GEN7-24191	Vulnerability involving improper neutralization of HTTP header resulting in unauthenticated DoS.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-18760, GEN7-19718, GEN7-20821, GEN7-21236, GEN7-22362, GEN7-22480, GEN7-22545, GEN7-23364, GEN7-23541, GEN7-23657, GEN7-23870, GEN7-23877, GEN7-23976

Known Issues

Issue ID	Issue Description
GEN7-23969	Not able to log in as a user with RADIUS authentication from the LAN zone.
GEN7-24521	On NSv, AWS VPN does not show VPC details.
GEN7-24608	The Cancel button does not work on the Capture ATP Location page.
GEN7-24639	Traffic still passes after blocking LAN to LAN HTTP in Access Rules after enabling firewalling with other bridge members.
GEN7-24658	Configuration changes in TOTP (2FA) result in a full sync and reboot of non-primary blades and can cause temporary access issues.
GEN7-24683	Exported CSV file has no data when security policies are sorted by group.

Version 7.0.1 April 2021

April 2021

SonicOS 7.0.1 introduces support for the SonicWall NSa 3700 network security appliance. This release provides several new features and enhancements, and fixes a number of issues found in previous releases.

Compatibility and Installation Notes

SonicOS 7.0.1 supports all the features and contains all the resolved issues in previous releases of SonicOS 7.0.

- **Browser Compatibility** – SonicWall recommends using the latest Chrome, Firefox, Safari, or Edge browsers for administration of SonicOS. Incognito and private mode are not supported.
- **Product Licensing** – A MySonicWall account is required. SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support.
- **Wireless WAN** – 4G/LTE devices are supported on SonicWallTZ and NSa Series firewalls. To see a list of supported devices, go to: Wireless-cards-and-broadband-devices-supported-on-sonicwall-firewalls-and-access-points
- **Cloud Management** – Network Security Manager (NSM) 2.2 supports management of all SonicWall firewalls running 7.0.1.

Supported Platforms

SonicOS 7.0.1 is supported on the following SonicWall network security appliances:

- NSa 2700
- NSa 3700
- NSsp 15700
- TZ270 / TZ270W
- TZ370 / TZ370W
- TZ470 / TZ470W
- TZ570 / TZ570W
- TZ570P
- TZ670
- NSv 270
- NSv 470
- NSv 870

NSv 270/470/870 deployments are supported on the following platforms:

- AWS (BYOL or PAYG)
- Microsoft Azure
- VMware ESXi

- Microsoft Hyper-V
- Linux KVM

What's New

- **Support for Auth Code during SafeMode Authentication**

  You can use the appliance Auth Code as the Maintenance Key when accessing SafeMode on unregistered firewalls running SonicOS 7.0.1. The Auth Code is displayed in the web management interface and on the label affixed to the bottom of the appliance.
- **Switch Integration:**
  - **Native VLAN configuration** support in SonicOS for SonicWall Switches

    Provides ability for administrator to specify which VLANs do not carry a VLAN tag. This helps with SonicWave provisioning.
  - **New Port Description field** for each switch port provides easy labeling of ports
  - **Eight Switches per firewall** are supported, up from four Switches in previous releases
  - **Support for multiple standalone Switches** for SonicWall firewall High Availability deployments
- **SDWAN support on Root Instance** of NSsp15700
- **One-Arm Mode** interface support for NSv private cloud deployments on VMware, Hyper-V and KVM platforms

  In One-Arm Mode, traffic enters and leaves the appliance on the same interface.
- **PPPoE interface mode support** on NSv 270/470/870
- **SR-IOV NIC support** on NSv 270/470/870 deployed on KVM platforms

  The Single Root I/O Virtualization (SR-IOV) PCI standard allows virtual machines to share access to a physical network interface card (NIC) installed in the hypervisor.
- **Bootstrap configuration provisioning support** for NSv 270/470/870 on KVM platforms
- **Firmware upgrade support from NSv 7.0.0** firmware version to NSv 7.0.1 in Policy Mode
- **SonicOS Classic Mode availability on NSv** 270/470/870:
  - Firewall Mode switching available between Classic and Policy Mode
  - Firewall Mode switching option on the NETWORK | Firewall > Advanced page
  - Firewall Mode switching option in MySonicWall controls visibility of this option on the firewall, must be enabled for the NSv serial number in the MySonicWall account
  - Firewall Mode choice of Classic or Policy Mode for new SonicOS 7.0.1 NSv deployments
  - Fresh NSv 7.0.1 deployments in Classic Mode support settings imports from NSv 6.5.4.v instances

Resolved Issues

Issue ID	Issue Description
GEN7-9974	On TZ Series platforms, the administrator cannot modify the Account Expires option in a Guest account using time increments expressed in units (Days, Hours, or Minutes) other than the unit used in the original configuration.
GEN7-10226	With Client DPI-SSL enabled, when the SSL client uses ECDHE-ECDSA cipher suites to connect towebsites which support TLS1.3 such as Facebook, the connection cannot be established.
GEN7-10783	On NSv or TZ firewalls, the Audit Log is incorrect or missing information when importing a configuration settings file.
GEN7-12366	On NSv or TZ firewalls, an excluded user setting within a DENY access rule does not work.
GEN7-13697	When using DHCP over VPN on a VLAN interface, if bound to a VLAN interface in unassigned state, the peer cannot decrypt packets.
GEN7-15097	Percentage-Based WAN Load Balancing does not work as expected. Running the traffic flow based on user defined Percentage-Based WAN Load Balancing fails with existing/previous traffic flows.
GEN7-15344	NSsp 15700 does not show Network Monitor Object in Routing rule and Probe drop-down list.
GEN7-15352	When using Single Sign-On on an NSsp 15700, the option for Partition selection is not available when adding an SSO agent.
GEN7-15601	When Single Sign-On is toggled in the SSO Agent, RADIUS accounting packets are consistently dropped by the firewall rule. Because of this, the SSO Agent keeps trying to connect and keeps failing.
GEN7-15646	On NSv series platforms, SSH management of the firewall fails when the SSH port is configured to use a non-standard port.
GEN7-15672	On NSv series platforms, the web management interface hangs after deleting the DoS action profile that is used by a DoS policy.
GEN7-16351	On an NSsp 15700 with Authentication Partitioning enabled, the LDAP server does not have a partition setting. When adding or editing an LDAP server, there is no Partition field or setting.
GEN7-16659	On NSv series platforms, the product code and model name are not displayed in the SonicOS/X web management interface and management console after registration using an NSv serial number if the serial number has never been registered before. If the serial number has been registered by someone (even if this SN has been deregistered), this issue does not occur. Restarting the NSv after registration will also solve this issue.
GEN7-16824	On TZ series platforms, the Prevention and Detection settings for many IPS signatures are not consistent by default with the category settings.

Issue ID	Issue Description
GEN7-17413	On an NSsp 15700 High Availability pair, the standby firewall loses web and console responsiveness when Virtual MAC is disabled on the active firewall with Override MAC Address enabled.
GEN7-17546	On NSsp 15700, FTP packets are dropped when using FTP through a VPN tunnel.
GEN7-17566	On a TZ470 after upgrading firmware, the X8 and X9 interfaces display "NO LINK" and are down.
GEN7-17664	With Client DPI-SSL enabled, changing the re-signing certificate does not take effect without rebooting the firewall.
GEN7-17929	When editing Access Rules on SonicOS 7.0, the Bandwidth Management profiles are set to Disabled by default and the error message, "Error: property 'bandwidth_management' can't be empty object" is displayed on the first attempt to apply a rule.
GEN7-18021	In a High Availability pair with Enable Stateful Synchronization selected, attempting to use the Tools & Monitors > Active Connections page results in an error popup message, "HA idle".
GEN7-18025	When attempting to delete a custom zone that is no longer used in any interface, an error message displays, "Object is in use by an Access Rule."
GEN7-18035	On an NSa 2700, no link is established when connecting a 10 GB SFP+ module on interface X18 to a SonicWall Switch.
GEN7-18097	An NSv for Hyper-V deployed on Windows server 2019 cannot boot up successfully when clicking "factory default" in the management console.
GEN7-18381	The DNS settings cannot be saved when configuring IPv6 options under Specify DNS Servers Manually on the NETWORK | DNS > Settings page.
GEN7-18457	On an NSa 2700 with more than 40,000 Single Sign-On user sessions, the web management interface hangs for about 3 minutes after navigating to the DEVICE | Users > Status page.
GEN7-18553	On an NSa 2700, moving the native bridge mode of an interface to a LAN interface causes a segmentation fault.
GEN7-18562	On a TZ670 with Link Aggregation configured, traffic fails after shutdown of the Parent Interface of a static LAG.
GEN7-18651	On an NSa 2700 with multiple Switches portshielded to the firewall X0 interface and active client connections, traffic flow does not resume after restarting the firewall.
GEN7-18654	On an NSa 2700 with multiple Switches connected, the firewall sometimes goes down when trying to delete Switches.
GEN7-18734	A backed up configuration with X1 in DHCP mode but without an IP address cannot be imported when attempting to reboot the firewall with that saved configuration, resulting in a failed reboot attempt.
GEN7-18775	On an NSa 2700 High Availability pair, toggling Preempt mode on the active firewall causes the standby firewall to reboot.

Issue ID	Issue Description
GEN7-18927	On an NSa 2700, the default management IP address for the MGMT port cannot be changed, and the error message, "Command no one arm mode does not match" is displayed.
GEN7-18958	On an NSa 2700 using the classic navigation view, the PortShield Groups page is missing.
GEN7-19039	An error popup, "Network error", is displayed after exporting configuration settings on a firewall with connected SonicWall Switches and then rebooting with factory defaults and importing the saved settings file, although the settings are successfully imported after some time.
GEN7-19255	On an NSsp 15700, login fails after importing configuration settings that were exported from the same NSsp.
GEN7-19741	An NSa 3700 reboots multiple times and the traffic interface ports go down with "NO LINK" displayed for ports X28 and X29.
GEN7-19767	On an NSv for Azure Active/Standby High Availability deployment, the firmware cannot be upgraded.
GEN7-19886	On NSv series, the WAN interface cannot be configured in PPPoE mode due to the error "Schema validation error: unknown property 'pppoe'".
GEN7-19970	On an NSv AWS PAYG (Pay as you Go) instance, the LAN to WAN traffic cannot be matched with the respective LAN to WAN security policy if Gateway AntiVirus is enabled in the action profile before the NSv AWS instance is associated in MySonicWall.
GEN7-20062	Before registering an NSv AWS PAYG instance, Capture Threat Assessment report generation displays an incorrect error message and fails to generate the CTA report.
GEN7-20280	On an NSa 2700, the power button does not work with a long press after using a short press to shut down the system. Short Press takes less than 5 seconds, while Long press needs more than 5 seconds.
GEN7-20315	On an NSa 2700 with more than 40,000 Single Sign-On users, clicking on Users > Status > Show Count results in an unknown error.
GEN7-20316	On an NSa 2700 with more than 40,000 Single Sign-On users, an error is displayed while trying to change Access Rules: "Error: unknown property 'block_traffic_for_single_sign_on'".
GEN7-20673	The IPv6 Default LB Group of an interface already configured as part of Failover & LB incorrectly allows some settings to still be configurable.
GEN7-20752	High Availability cannot be configured if the standby/peer serial number was once wrongly specified.
GEN7-21397	On NSsp 15700, files transferred using SMB are not sent to Capture ATP for analysis.
GEN7-21398	On NSsp 15700, .zip archive type files are not sent to Capture ATP for analysis.
GEN7-21486	On NSsp 15700, enabling Enhanced Security resulted in no files being sent to the Capture ATP engine.

Issue ID	Issue Description
GEN7-21582	On NSsp 15700, Block Until Verdict does not block malicious file download over HTTP/HTTPS with DPI-SSL enabled.
GEN7-21741	SonicOS (Policy Mode) does not support the common ‘real-world’ use case where 5-tuple matches multiple security (ULA) policies with differing (but partially overlapping) web categories applied in a positive matching allow action, unless it applies to non-referrer type websites which are rated with one or multiple categories in the applied group.
GEN7-21799	Packets with length larger than 1522 bytes cannot be received when Jumbo Frame is enabled on NSa 2700/3700 firewalls and the interface's MTU has been set to 9000.

Additional References

The following additional resolved issues in this release are listed here for reference:

GEN7-14373, GEN7-15097, GEN7-18103, GEN7-18280, GEN7-18494, GEN7-18585, GEN7-18591, GEN7-18634, GEN7-18666, GEN7-18730, GEN7-18760, GEN7-19009, GEN7-19086, GEN7-19355, GEN7-19384, GEN7-19404, GEN7-19459, GEN7-19460, GEN7-19529, GEN7-19537, GEN7-19546, GEN7-19559, GEN7-19593, GEN7-19606, GEN7-19612, GEN7-19619, GEN7-19649, GEN7-19650, GEN7-19659, GEN7-19721, GEN7-19777, GEN7-19820, GEN7-19830, GEN7-19974, GEN7-20038, GEN7-20050, GEN7-20110, GEN7-20124, GEN7-20204, GEN7-20246, GEN7-20247, GEN7-20366, GEN7-20411, GEN7-20414, GEN7-20510, GEN7-20517, GEN7-20544, GEN7-20601, GEN7-20699, GEN7-20708, GEN7-20766, GEN7-20821, GEN7-20856, GEN7-20866, GEN7-21036, GEN7-21047, GEN7-21069, GEN7-21082, GEN7-21094, GEN7-21225, GEN7-21234, GEN7-21235, GEN7-21236, GEN7-21310, GEN7-21320, GEN7-21321, GEN7-21323, GEN7-21357, GEN7-21358, GEN7-21360, GEN7-21363, GEN7-21393, GEN7-21400, GEN7-21438, GEN7-21445, GEN7-21464, GEN7-21490, GEN7-21493, GEN7-21555, GEN7-21556, GEN7-21558, GEN7-21592, GEN7-21728, GEN7-21742, GEN7-21771, GEN7-21773, GEN7-21774, GEN7-21880, GEN7-21917, GEN7-22007, GEN7-22055, GEN7-22084, GEN7-22151, GEN7-22194, GEN7-22236, GEN7-22277, GEN7-22353, GEN7-22358, GEN7-22391, GEN7-22423, GEN7-22443, GEN7-22600, GEN7-22652, GEN7-22775, GEN7-22787, GEN7-23040

Known Issues

Issue ID	Issue Description
GEN7-16351	On NSsp with Authentication Partitioning enabled, there is no Partition field or setting when adding or editing an LDAP server.
GEN7-19930	High Availability settings are lost, but other settings are retained when importing configuration settings to an NSa 2700 that were exported from an NSa 2600 running SonicOS 6.5.4.7.

Issue ID	Issue Description
GEN7-21228	A client PC cannot obtain a DHCP IP address in certain deployments involving IP Helper over an unnumbered tunnel VPN. Occurs when an unnumbered tunnel VPN is established between two firewalls, where FW1 is a DHCP server and FW2 has IP Helper enabled, and the client PC is connected to FW1.
GEN7-21977	Adding, deleting and configuring or managing Dell X series switches on an NSa 3700 is not working as expected and the error message, "Error: Index of the Extended Switch Instance" is displayed.
GEN7-22151	During SonicOSX web management, the browser might display the error "Failed to open cache db". This occurs because SonicOSX web management is not supported from browsers in private or incognito mode, including Firefox, Chrome and Edge. **Workaround**: Manage the firewall using a browser in normal mode.
GEN7-22269	An error pops up saying, "Unknown Reason" when accessing the firewall in non-configuration/readonly mode and attempting to select or clear the check box of any option, such as on the Users > Local Users & Groups > Settings page. A more descriptive error message should be displayed.
GEN7-22706	When deploying multi-level Switch daisy chaining, it takes more than five minutes to detect a Switch at the third level. That is, after connecting it to a Switch that is already connected with daisy chaining to a Switch connected to the firewall.
GEN7-22772	The VLANs of the parent Switch are not properly configured on the child Switches in multi-level daisy chaining.
GEN7-22807	Client connections consistently fail with "Timeout" log messages when attempting to connect to a firewall with SSL VPN Server enabled.
GEN7-22950	After registering the firewall using the manual license keyset method and entering the license keyset, the security services Signature File ID (SFID) is incorrect when checked on the POLICY | Security Services > Summary page under UPDATE SIGNATURES MANUALLY.
GEN7-22972	When using SSH Terminal, a LAN PC cannot connect to an SSH session after disabling and then enabling SSH management on the X0 interface.
GEN7-23108	X1 cannot be enabled administratively after an NSv is registered using the manual keyset.
GEN7-23121	On NSsp, Instances sometimes stop working soon after firmware upgrade. This occurs when LDAP is enabled with multiple LDAP servers, due to an issue related to the LDAP referrals. **Workaround**: Disable LDAP referrals in SonicOS.
GEN7-23131	In a Stateful High Availability deployment, the standby unit sometimes stops working after adding, editing or deleting a CFS Custom Category.
GEN7-23165	On NSv, inbound "Deny" access rules from WAN to WAN for HTTPS Management access sometimes do not block traffic.
GEN7-23211	On NSv, the Protocol tab/screen is not available when editing an interface with Zone set to WAN and Mode / IP Assignment set to PPPoE.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

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

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

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

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

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

SonicOS Release Notes
Updated - August 2024
Software Version - 7.0
232-005596-00 Rev ZF

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.