SonicOS and SonicOSX 7.0.0

Release Notes

October 2020

These release notes provide information about the SonicWall SonicOS and SonicOSX 7.0.0 release on SonicWall TZ Series and NSsp 15700 firewalls.

Topics:

About SonicOS and SonicOSX 7.0.0

SonicOS/X 7.0.0 is a maintenance release on SonicWall Gen 7 TZ Series and NSsp 15700 firewalls. This release resolves a number of issues found in previous releases of SonicOS/X.

See the Supported Platforms and Resolved Issues section for more information.

Supported Platforms

SonicOS 7.0.0 is supported on the following SonicWall TZ Series firewalls:

- TZ670
- TZ570
- TZ570P
- TZ570W

SonicOSX 7.0.0 is supported on the following SonicWall NSsp firewalls:

- NSsp 15700

Resolved Issues

This section provides a list of resolved issues in this release.

Resolved Issue Description	Issue ID
The **Local Capture ATP Analysis** option is missing from the Policy | Capture ATP > Settings page.	GEN7-12014
A 10 Gbps link between the TZ670 and the SonicWall Switch does not pass traffic. Connectivity on the 10 Gbps link between TZ670 SFP+ ports and SWS14-48 switches does not work when the TZ670 interface speed is configured to 10 Gigabit Full Duplex.	GEN7-13382
After adding an SSL server and then changing a DPI-SSL Server base setting such as Enable/Disable DPI-SSL Server or excluding an IP address, the added SSL server disappears.	GEN7-14156
A search for an LDAP user fails with error message, "Cannot read property 'message' of undefined".	GEN7-14423
The error message "Command 'no network-address ipv6' does not match" is displayed when configuring SSLVPN Client settings.	GEN7-14706
The SSO service bypass or address bypass options cannot be configured if the object name contains a forward slash character ('/').	GEN7-14864
Editing, disabling, and deleting an App Rule does not work. An error message pops up and the rule is unchanged and remains in the rule list.	GEN7-14995
No resolved IP address is displayed when the IPSec gateway is specified as the domain name.	GEN7-15051
An error occurs when testing "Check User" connection of SSO Agent.	GEN7-15098
The RADIUS status does not show the active icon (green) after adding a valid RADIUS server.	GEN7-15164
Unable to configure Access Rules from the web management interface if Source and Destination addresses are specified, rather than both set to ANY.	GEN7-15702
The **Use RADIUS in** option under IPSec VPN > Advanced cannot be enabled, preventing GVC users from logging in with RADIUS authentication. The option is	GEN7-16785

Resolved Issue Description	Issue ID
misplaced in the UI and the user is meant to select one of the choices below it.	
Settings on the SSLVPN > Server Settings page cannot be saved and the error message "Custom URL can not be null" is displayed.	GEN7-17127

Known Issues

This section provides a list of known issues for this release.

Known Issue Description	Issue ID
HTTPS downloads do not start on a client machine if Bandwidth Management is enabled in an App Rule and Client DPI-SSL is enabled for Application Firewall. **Workaround**: Disable DPI-SSL.	GEN7-3971
When managed through TZ Series firewalls, SonicWall Switches do not support Jumbo Frames. **Workaround**: Do not enable Jumbo Frames when managing the Switch through a TZ firewall.	GEN7-9148
After releasing and renewing DHCPv6 addresses , old IPv6 addresses still show on the web management interface.	GEN7-9271
Explanation is needed on System Alert messages.	GEN7-9509
PPTP client cannot initiate a new call after a PPTP Call-Disconnect-Notify.	GEN7-9575
With DPI-SSL Client enabled, when an SSL client uses ECDHE-ECDSA cipher suites to connect to websites which support TLS 1.3, such as Facebook, the connection cannot be established. **Workaround**: SSL client can use other cipher suites besides ECDHE-ECDSA.	GEN7-10226
On the DEVICE | Log > Settings page, the Template > Import From Template action returns an error. **Workaround**: Log into the legacy management interface, then perform the action.	GEN7-10515
Configuring multiple Switch ports is not pushed using a single command, and therefore consuming a lot of time.	GEN7-10557
The peer cannot decrypt packets coming from the VPN tunnel. Occurs when using DHCP over VPN on a VLAN interface, if bound to a VLAN interface in unassigned state. **Workaround**: Assign an IP address to the VLAN bound-to interface on the remote peer.	GEN7-13697
Auto-negotiation of link speed does not work with some SFP types, such as NBASE-T or TWINAX SFP. **Workaround**: Manually select the link speed in SonicOS.	GEN7-14558
Percentage-based WAN Load Balancing is not working as expected.	GEN7-15097

Known Issue Description	Issue ID
Occurs when X3 is configured as Primary WAN and X1 as secondary WAN and both are in default WAN Failover IPv4 Group with Load Balancing Method = Ratio [X3 = 95% and X1 = 5%]. X1 still carries most of the traffic.	
Tenant firmware upload fails from the MGMT port on the NSsp 15700.	GEN7-15305
A TZ 570W stops reporting data to NSM after 1 to 3 hours until toggling the VPN off and then on again.	GEN7-15587
The Exclude common name option in DPI-SSL Client does not work as expected. When trying to access excluded websites, they are shown with an incomplete display and cannot be logged into. For example, occurs when DPI-SSL Client and CFS are enabled and CFS is configured to block the Shopping category, and then shopping websites are added to the DPI-SSL Client exclude common name option.	GEN7-16352
The DNS server settings in **Specify DNS Servers Manually** cannot be saved.	GEN7-16505
An error occurs when clicking the **Test capture ATP connectivity** .	GEN7-17530
Editing an Access Rule fails and an error message pops up. Occurs after enabling egress and ingress BWM and then disabling them.	GEN7-17611
SonicOS/X does not show the proper error message when the Dynamic External Object downloaded address objects exceeds the maximum count. **Workaround**: Make sure the number of address objects in the external object file (int http/ftp server) does not exceed the maximum.	GEN7-17628
The subnet information is not displayed for the downloaded external address object in the Dynamic Group page.	GEN7-17671
Cannot create VPN with an underbar ('_') character in the Shared Secret. **Workaround**: Do not use an underbar ('_') character in the Shared Secret.	GEN7-17740
Unable to enable WAN Group VPN if **Virtual Adapter** is set to "DHCP lease" or "DHCP or Manual configuration" after importing the configuration settings EXP file from a TZ600.	GEN7-17770
Data in the Capture ATP Dashboard and Scanning History pages is still read from Cloud Capture ATP when Local Capture ATP Analysis is selected.	GEN7-17913
An M2100 modem does not connect again after the firewall reboots.	GEN7-18011
Changing the Syslog Facility value to a different value for the syslog server does not change the Syslog Facility value to Mixed on Syslog Settings segment.	GEN7-18020
The standby device in a High Availability pair cannot use the Active Connections feature and displays the message "HA idle".	GEN7-18021
The error message "Object is in use by an Access Rule: is displayed when deleting a custom zone which was previously used in the settings for an interface which was then changed to another zone.	GEN7-18025
The Raw mode tab is not present for Junk Box email messages. **Workaround**: Download the message as an .eml file from the SonicOS or Junk Store user interface and view the source in a text editor.	ES-5052

System Compatibility

This section provides additional information about hardware and software compatibility with this release.

- **Wireless 4G/LTE Broadband Devices**

  4G/LTE devices are supported on SonicWall TZ Series firewalls.

  SonicOS/X 7.0.0 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see:

  https://www.sonicwall.com/support/knowledge-base/what-wireless-cards-and-broadband-devices-aresupported-on-sonicwall-firewalls-and-access-points/170505473051240/

- **Network Security Management Support**

  Management of SonicWall TZ Series firewalls running SonicOS/X 7.0.0 requires Network Security Manager 2.0 or higher.

  NSv and NSsp firewalls running SonicOSX 7.0.0 currently cannot be managed by SonicWall GMS, CSC-MA, or NSM.

- **Browser Support**

  SonicWall recommends using the latest Chrome, Firefox, Safari, or Edge browsers for administration of SonicOS/X. This release supports the following web browsers:

  - Google Chrome
  - Mozilla Firefox
  - Apple Safari
  - Microsoft Edge

  ⓘ | **NOTE:** Microsoft Internet Explorer (IE) is **not** supported for management of SonicOS/X 7.0.0.

Product Licensing

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. Log in or register for a MySonicWall account at https://mysonicwall.com.

Upgrading Information

- **TZ Series:**

  For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall TZ Series appliance, and importing configuration settings from another appliance, see the *SonicOS/X 7.0 Upgrade Guide* available on the Support portal at https://www.sonicwall.com/docs/tz

  Existing settings for **Global Bandwidth Management**, **Virtual Assist** and **Content Filter Client Enforcement** cannot be imported into SonicOS/X 7.0.0. Global Bandwidth Management is replaced by Advanced Bandwidth Management, and the other features are deprecated in SonicOS/X 7.0.0. For more information about configuring Advanced Bandwidth Management, refer to the knowledgebase article *How Can I Configure Advanced Bandwidth Management On Gen 7?* at: https://www.sonicwall.com/support/knowledge-base/how-can-i-configure-advanced-bandwidth-management-on-gen-7/200818093436630/

  Refer to the *SonicOS/X 7.0 Upgrade Guide* for details about importing configuration settings from previous generation TZ firewalls to SonicWall TZ670/TZ570 Series firewalls.

- **NSsp Series:**

  You can upgrade your NSsp from SonicOSX if it is running a previous build of SonicOS/X 7.0.0. You can download the latest firmware from MySonicWall at https://www.mysonicwall.com.

  Neither upgrading nor importing configuration settings from NSsp platforms running SonicOS 6.5 or earlier to NSsp appliances running SonicOSX 7.0.0 is supported in this release.

SonicWall Support

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

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

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

About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

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

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

SonicOS and SonicOSX Release Notes
Updated - October 2020
Software Version - 7.0.0
232-005381-00 Rev E