

Dell™ SonicWALL™ SonicOS 6.2.5.2

Release Notes

October 2016, updated November 2016

These release notes provide information about the Dell™ SonicWALL™ SonicOS 6.2.5.2 release.

Topics:

- [About SonicOS 6.2.5.2](#)
- [Supported platforms](#)
- [IPv6 support](#)
- [Resolved issues](#)
- [Known issues](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading information](#)
- [Technical support resources](#)
- [About Dell](#)

About SonicOS 6.2.5.2

The SonicOS 6.2.5.2 release provides important updates with fixes for many issues found in previous releases. See [Resolved issues](#) for descriptions covering many of these fixes.

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 6.2.5.x. For more information, see the previous release notes, available on MySonicWALL or on the Support Portal at: <https://support.software.dell.com/release-notes-product-select>.

TZ Series / SOHO Wireless feature support

Dell SonicWALL SOHO Wireless and TZ series appliances running SonicOS 6.2.5.2 support most of the features available for other platforms. Only the following features are *not* supported on the TZ series or SOHO Wireless appliances:

- Active/Active Clustering
- Advanced Switching
- Jumbo Frames
- Link Aggregation
- Port Redundancy
- Wire Mode

In addition, SOHO Wireless appliances do not support the following features:

- App Visualization (Real-Time Monitor and AppFlow)
- Geo-IP Filtering
- Botnet Filtering
- High Availability

Supported platforms

SonicOS 6.2.5.2 is supported on the following Dell SonicWALL network security appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 and TZ500 Wireless
- TZ400 and TZ400 Wireless
- TZ300 and TZ300 Wireless
- SOHO Wireless

IPv6 support

For the features supported with IPv6 in this release, see the *SonicOS 6.2.5 IPv6 Support Reference Guide*, available on the Support portal page for any appliance platform that can run SonicOS 6.2.5. For example, see:

<https://support.software.dell.com/sonicwall-nsa-series/release-notes-guides>

Resolved issues

The following issues are resolved in this release.

High Availability

Resolved issue	Issue ID
Default zones such as those for DMZ or VPN disappear on the firewall or on the secondary device in a High Availability pair. Occurs on TZ series and NSA 2600 firewalls when there are custom zones configured on the firewall(s) and then configuration settings are imported or an HA failover occurs.	176050

Networking

Resolved issue	Issue ID
<p>A Network Monitor policy in an exported preferences file is not imported when the preferences file is imported.</p> <p>Occurs when several different policies are created (such as Network Monitor and NAT policies) and then subsequently exported to a preferences file. When the firmware is then booted with factory defaults and the preferences file is imported, the first Network Monitor policy created is not included with the rest of the policies in the file.</p>	177886
<p>The firewall has high CPU utilization associated with RST Flood events in the log and dropped TCP packets on some connections.</p> <p>Occurs when running SonicOS 6.2.5.1 with certain traffic types which have unusual TCP behaviors, such as clients or servers which are not compliant with certain RFCs.</p>	173655
<p>An extended switch access VLAN configuration is not properly assigned.</p> <p>Occurs when a subinterface with a VLAN is created on a TZ appliance with an extended switch and either a common uplink or a switch uplink with a dedicated link. The extended switch is portshielded to the port with the VLAN configuration. When checking the extended switch, the VLAN configuration is assigned to some other VLAN supported in the dedicated uplink.</p>	170434
<p>PPPoE connections keep dropping approximately every 5 minutes.</p> <p>Occurs when Disconnect the PPPOE client if the server does not send traffic for <5> minutes is enabled on the Protocol tab of the Edit Interface dialog under Network > Interfaces.</p>	170017
<p>Displaying the Groups tab on the Network > PortShield page is excessively slow.</p> <p>Occurs when two X-Series switches are provisioned on a TZ series appliance and then one switch is removed from the user interface of the appliance. The setting is exported and saved from the System > Settings page. When importing the saved settings, the display of the Groups tab is excessively slow.</p>	169847

SSL VPN

Resolved issue	Issue ID
<p>Virtual Office users are logged out unexpectedly and without notification.</p> <p>Occurs when the Show user login status window and Enable disconnected user detection options in the User Session Settings for Web Login section on Users > Settings are enabled and User's login status window sends heartbeat every (seconds) is set to 10 seconds. This does not stop existing RDP sessions, but does prevent new ones and does log the user out.</p>	177805
<p>Virtual Office does not show all data, buttons, or bookmarks.</p> <p>Occurs when a user attempts to log in to the Virtual Office portal. The portal remains mostly blank.</p>	172554
<p>Configuring a VLAN ID causes the page to display "Bad Request: The client issued a bad request."</p> <p>Occurs when Enter is pressed on the keyboard to configure a VLAN ID.</p>	170036

System

Resolved issue	Issue ID
<p>Both firewalls in a High Availability pair restart frequently due to data plane core exceptions. High CPU usage of about 80% is also occurring.</p> <p>Occurs when Active/Active DPI is enabled on an HA pair running SonicOS 6.2.5.1.</p>	173754

Resolved issue	Issue ID
<p>SNMPv3 stops working with the log message, "Invalid SNMP packet, Invalid engineID: 0, Error ID: 1220, Category System, Group SNMP, Msg Type 8."</p> <p>Occurs when the firewall is rebooted while SNMPv3 is enabled, and the subsequent SNMPv3 handshake query contains an incorrect (perhaps cached) engineTime, but the firewall does not respond as expected per the RFC.</p>	172987
<p>High CPU is seen across all data plane and control plane cores, and unexpected failovers occur in a High Availability pair. The SonicOS management interface and wireless access become unresponsive.</p> <p>Occurs when there is heavy traffic and Single Sign-On is enabled, and many "conn handle" trace log messages are generated.</p>	172486
<p>The 10 gigabit links on ports X16, X17, X18 and X19 can go down after a failover. The ports are fine again after administratively bringing them down and then up.</p> <p>Occurs when two SuperMassive 9000 series are connected as a High Availability pair with ports X16, X17, X18 and X19 configured in Wiremode and then a failover is forced during testing.</p>	166758

User Interface

Resolved issue	Issue ID
<p>Options for Power Over Ethernet are displayed for non-PoE Dell X-Series extended switches.</p> <p>Occurs when configuring a non-PoE extended switch and viewing the Advanced tab of the Add External Switch dialog.</p>	171573
<p>Dynamic pages, such as Dashboard > Log Monitor, Network > Address Objects, or Network > NAT Policies, cannot be loaded with the Microsoft Edge browser.</p> <p>Occurs when the Microsoft Edge browser is used. If the browser window is maximized, the page is blurred; if the browser window is not maximized, the page disappears.</p>	169277

Users

Resolved issue	Issue ID
<p>Guest services login and Users Licensing Agreement (ULA) pages do not display properly.</p> <p>Occurs when a guest user tries to authenticate access to a website. One of the following occurs:</p> <ul style="list-style-type: none"> The authentication page is not displayed. The authentication page displays, but after the user enters login/authentication details, the ULA popup page does not display. The ULA popup page displays, but the guest user is not redirected to the correct website. 	172902

VPN

Resolved issue	Issue ID
<p>Citrix and VoIP traffic over a Site-to-Site tunnel is disrupted and dropped during IKEv2 key renegotiation. Citrix clients have to reconnect manually.</p> <p>Occurs on firewalls running SonicOS 5.8.1.5 or 5.8.1.6, and on NSA 2600 firewalls after upgrading firmware to SonicOS 6.2.5.1. Traffic is dropped due to excessive time (for example, 3 - 5 minutes) required for tunnel renegotiation.</p>	174319

Resolved issue	Issue ID
An IPv6 manual key cannot be added, and a JavaScript error is displayed. Occurs when attempting to add an IPv6 manual key on the VPN > Settings > VPN Policy dialog.	170547
Any unnumbered tunnel interface with dynamic routing is not retained during an upgrade. Occurs when SonicOS 6.x is upgraded to SonicOS 6.2.5.1.	169993

Wireless

Resolved issue	Issue ID
Authentication for a SonicPoint ACe/ACi/N2 cannot be changed directly. Occurs when changing the authentication type from WPA2 - EAP to WEP - Shared Key when configuring the profile for a SonicPoint ACe/ACi/N2.	171722
Guest WiFi users cannot access the Internet. Occurs when X0 (LAN) is bridged to another interface, such as X7, to which a SonicPoint is connected.	171199

Known issues

This section contains a list of known issues in this release.

3G/4G

Known issue	Issue ID
A Sprint 341U card takes more than 10 minutes to connect. Occurs when the Sprint 341U is connected to U0, which is configured as the Final Backup with a 4G profile, and then failover from the Primary WAN (X1) is triggered by unplugging the cable from X1.	166381
A Huawei E182E 3G card is not properly detected by SonicOS and cannot connect. The console shows that the card is detected, but the SonicOS web management interface shows "No device". The U0 interface is not shown as final backup, but appears in an alternate group. Occurs when the Huawei E182E 3G device is functioning properly at first, U0 is configured as final backup for the WAN in persistent mode, and the X1 interface is disconnected just before the appliance is restarted while the device remains inserted.	164232
It takes U0 between 4-6 minutes to reconnect after the data limit is reset. Occurs with AT&T Beam, Verizon 290, Sprint 760, and AirCard 340U when U0 is the final WAN backup in Persistent mode with 100K data limit, and after failover to U0 the data limit is reached and then the administrator resets the data limit on the 3G/4G > Data Usage page.	160190
Huawei 3G cards do not connect to the Internet after the X1 WAN interface is disconnected. Occurs when one of several Huawei 3G cards is inserted in the TZ appliance and the U0 interface is configured as the Final Backup in the Network > Failover & LB page.	159273

Application Control

Known issue	Issue ID
<p>The Ultrasurf browser plugin is not blocked by an App Rule or App Control Advanced policy.</p> <p>Occurs when using the Chrome browser plugin for Ultrasurf.</p>	161651
<p>App Control does not block access to Google Play app store from a smartphone app, but play.google.com is blocked from a browser on a personal computer.</p> <p>Occurs when DPI-SSL is not enabled and an App Rule is configured on the firewall to block the Google Play application and signatures, then an Android smartphone connects to the firewall via a wireless access point and can download or update apps from the Google Play store.</p>	157692
<p>App Control Advanced does not block the Psiphon client version 95 or 87.</p> <p>Occurs when the Proxy-access category is enabled in App Control Advanced along with signatures 5, 6, and 7, with or without DPI-SSL enabled, and with or without a rule to block UDP ports 500 and 4500.</p>	151710

Bandwidth Management

Known issue	Issue ID
<p>An Advanced BWM policy works for egress traffic, but not for ingress traffic.</p> <p>Occurs when two SonicPoints are connected to the same firewall interface and Advanced BWM policies are configured for both egress and ingress traffic between wireless clients of the two SonicPoints.</p>	178292

DPI-SSL

Known issue	Issue ID
<p>An internally hosted SSL web page loads very slowly. The web page pulls content from different internally hosted servers.</p> <p>Occurs when Server DPI-SSL is enabled on the firewall and the web page includes a reference to a JavaScript element, pack_99.js.</p>	173546
<p>HTTPS downloads are slow and either hang or fail. HTTPS sites load slowly and often fail to load. File transfers from Zone to Zone are slow and can fail, such as CIFS traffic.</p> <p>Occurs when Client DPI-SSL Inspection is applied to a host which is accessing HTTPS sites and downloading files over HTTPS.</p>	172063
<p>A NetExtender connection is disconnected.</p> <p>Occurs when HTTPS connections are initiated or files downloaded via SCP to a host on the other side of the SSL VPN connection.</p>	169379
<p>Client DPI-SSL does not inspect traffic on the WWAN interface. No messages, such as "connection is untrusted", are displayed when connecting to a secure website using HTTPS.</p> <p>Occurs when the firewall is using a 3G or 4G card for the WAN connection and Client DPI-SSL is enabled, but the default Dell SonicWALL DPI-SSL CA certificate is not installed on the browser.</p>	163672
<p>Applications such as YouTube are slow to load or do not load properly.</p> <p>Occurs when the DPI-SSL service is enabled and policies are configured with Advanced Bandwidth Management; the policies might not work as configured.</p>	158183

High Availability

Known issue	Issue ID
Failover occurs unexpectedly when the aggregator port goes down in a Layer 2 Link Aggregation Group, but the associated member port remains up. Occurs when the High Availability Active/Standby Failover only when ALL aggregate links are down option is enabled and only one port in the L2 LAG is down.	178299
HA Primary and Secondary firewalls are unavailable for a brief period during a manual configuration change and a restart of the Primary Firewall in Active state. Occurs when a configuration change is made on the Primary firewall in the Active state, and then the restart link on the SonicOS management interface status bar is clicked.	171787

Log

Known issue	Issue ID
Cannot modify a syslog server port. Occurs when trying to modify the syslog port from a GMS server.	160355
The source and destination of the App Rules log messages are reversed. The source is the real destination, and the destination is the real source. Occurs when viewing the App Rules log messages.	149458

Networking

Known issue	Issue ID
The Dell X-Series switch connected to a TZ series appliance is inaccessible and status is down after configuration of a dedicated link with just a MGMT uplink. Occurs when the X-Series switch is set up for Dynamic IP , thus receiving a new IP address when the DHCP server is enabled. Workaround: During the initial set up of the X-Series switch, be sure to choose Static IP instead of Dynamic IP .	170141
Portshielding X-Series switches on a TZ series appliance takes too long. Occurs when portshielding multiple ports in any combination to a PortShield group on any X-Series switch on a TZ series appliance. It takes 15 seconds to portshield each port. For example, to portshield 24 ports, it takes 15 seconds * 24 = 240 seconds = 6 minutes.	170026
The firewall cannot form full adjacency with all neighboring routers using OSPF. Occurs when OSPF is enabled on one interface of the firewall with router priority 200, which is connected to a test system running OSPF with 20 simulated neighboring routers, all with priority 0. Only about half of the neighbors are able to reach FULL status.	166564
An IPv6 BGP neighbor cannot be established. Occurs when both IPv6 and IPv4 BGP are configured on the network at the same time, and the IPv4 BGP is configured with authentication, but the IPv6 BGP is not configured for authentication.	157525
The firewall cannot enable OSPF through the console. Occurs when trying to enable the OSPF through the firewall console. The network needs to first match the OSPF wildcard bits.	153350
The firewall cannot enable RIPv2 through the console. Occurs when trying to enable RIPv2 through the firewall console and the subnet is not set, or the subnet is 32-bit as with 10.8.109.0 where the IP address last byte is 0.	153267

Known issue	Issue ID
The firewall learns OSPF routes from areas other than area0. Occurs when the network topology includes 3 firewalls with 3 areas, all with VLANs configured, and the OSPF routes are checked on the area1 firewall.	153096
There is no option to originate a default route for dynamic IPv6 routing via OSPFv3. Occurs when configuring OSPFv3 from the Network > Routing page. IPv6 default route origination via OSPFv3 is currently not supported.	150771

SSL VPN

Known issue	Issue ID
NetExtender cannot establish a connection from a client machine to the firewall. Occurs when the SYN Flood Protection Mode option under Firewall Settings > Flood Protection is set to Always proxy WAN client connections .	178937
Importing a certificate CRL file fails. Occurs when importing a certificate CRL file larger than 100KB.	169256

Switching

Known issue	Issue ID
The aggregated member interface of a Layer 2 Link Aggregation Group (LAG) fails to aggregate into the LAG after restarting the firewall. Occurs when the LAG aggregator interface and aggregated member interface are configured as trunk ports, each with a VLAN enabled, in the WAN zone using DHCP mode, and then the firewall is restarted.	167254

System

Known issue	Issue ID
Diagnostic reports cannot be sent from the firewall, and attempting to do so results in an incorrect log message, "Failed to send file to remote backup server, Error: 1, File:TSR". Occurs when using Send Diagnostic to Support from the System > Settings page.	163181

User Interface

Known issue	Issue ID
Firmware upgrade fails when uploaded through the SonicOS management user interface. Occurs when a firmware upgrade for a Dell X-Series 4012 extended switch is attempted through the SonicOS management interface. Workaround: Upgrade the switch firmware directly from the extended switch.	171763
The Dashboard > Real-Time Monitor display does not appear to work properly on TZ series appliances with X-Series switches. Occurs when X-Series switches are provisioned on a TZ series appliance. For example, a link between the TZ appliance and the X-Series switch configured as 10 Mbps is shown on the Dashboard > Real-Time Monitor as 100+ Mbps even though the link is working properly. As all the X-Series switch ports are portshielded, the data shown for these ports on the Dashboard > Real-Time Monitor is not applicable.	169000

VPN

Known issue	Issue ID
SonicWALL GMS, while running behind a gateway firewall, does not acquire a firewall for management, although an active VPN tunnel is created in the gateway device. Occurs when IPSEC Management Tunnel is selected as the Management Mode in the GMS settings configured from the System > Administration page on the managed firewall.	178775
After importing the configuration settings file from an appliance running 5.9.0.x or 5.9.1.0 to a TZ600 running 6.2.5.1, the interface to which the site-to-site VPN policy is bound changes from X1 to X0. Occurs when the configuration settings file on the VPN-bound interface is incompatible with 6.2.x.	143210

System compatibility

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

Wireless 3G/4G broadband devices

SonicOS 6.2.5.2 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see <http://www.sonicwall.com/supported-wireless-broadband-cards-devices/>.

GMS support

Dell SonicWALL Global Management System (GMS) management of Dell SonicWALL security appliances running SonicOS 6.2.5.2 requires GMS 8.1 service pack 1, which will be released in April.


WXA support


The Dell SonicWALL WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with Dell SonicWALL security appliances running SonicOS 6.2.5.1 or higher. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

Browser support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. Dell SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 9.0 and higher
- Safari 5.0 and higher running on non-Windows machines

 **NOTE:** On Windows machines, Safari is not supported for SonicOS management.

 **NOTE:** Mobile device browsers are not recommended for Dell SonicWALL appliance system administration.

Product licensing

Dell SonicWALL network security appliances must be registered on MySonicWALL to enable full functionality and the benefits of Dell SonicWALL security services, firmware updates, and technical support. Log in or register for a MySonicWALL account at <https://mysonicwall.com/>.

A number of security services are separately licensed features in SonicOS. When a service is licensed, full access to the functionality is available. SonicOS periodically checks the license status with the SonicWALL License Manager. The **System > Status** page displays the license status for each security service.

Upgrading information

For information about obtaining the latest firmware, upgrading the firmware image on your Dell SonicWALL appliance, and importing configuration settings from another appliance, see the *SonicOS 6.2 Upgrade Guide* available on MySonicWALL at <https://mysonicwall.com/> or on the Support portal at <https://support.software.dell.com/>.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to <http://software.dell.com/support/>.

The site enables you to:

- View Knowledge Base articles at:
<https://support.software.dell.com/kb-product-select>
- View instructional videos at:
<https://support.software.dell.com/videos-product-select>
- Engage in community discussions
- Create, update, and manage Service Requests (cases)
- Obtain product notifications

SonicOS Administration Guides and related documents are available on the Dell Software Support site at <https://support.software.dell.com/release-notes-product-select>.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit <http://www.software.dell.com>.

Contacting Dell


For sales or other inquiries, visit <http://software.dell.com/company/contact-us.aspx> or call 1-949-754-8000.


Copyright 2016 Dell Inc. All rights reserved.


This product is protected by U.S. and international copyright and intellectual property laws. Dell, the Dell logo, and SonicWALL are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

For more information, go to <http://software.dell.com/legal/>.

Legend

 **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.

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.