

# Dell™ SonicWALL™ SonicOS 6.2.5.3

## Release Notes

### November 2016

These release notes provide information about the Dell™ SonicWALL™ SonicOS 6.2.5.3 release.

Topics:

- [About SonicOS 6.2.5.3](#)
- [Supported platforms](#)
- [Resolved issues](#)
- [Known issues](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading information](#)
- [Technical support resources](#)
- [About Dell](#)

## About SonicOS 6.2.5.3

The SonicOS 6.2.5.3 release provides important updates with fixes for issues found in previous releases. See [Resolved issues](#) for descriptions covering 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 6.2.5.3 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 6.2.5.3 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

## Resolved issues

### Gateway Anti-Virus

| Resolved issue  | Issue ID |
|---|----------|
| Cloud Anti-Virus does not work on SonicOS 6.2.5.2.<br>Occurs when the appliance is updated to this level even when GAV is licensed and Cloud Anti-Virus signatures are available. | 179222   |

### GVC Client Setting

| Resolved issue  | Issue ID |
|---|----------|
| GVC users lose access to local resources after a few minutes of operation.<br>Occurs after connecting to the SonicWall network appliance using GVC. When trying to ping a local server, it times out after 1 or 2 minutes. Other IPs cannot be pinged either even though the GVC stays connected. | 178515   |

### Wireless

| Resolved issue   | Issue ID |
|--|----------|
| A SonicPoint endpoint stays in either <i>initializing</i> mode or <i>rebooting</i> mode.<br>Occurs when the SonicPoint is connected on WLAN Tunnel Interface and managed through Layer3. | 179973   |

# 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.<br>Occurs when the Sprint 341U is connected to U0, which is configured as the <b>Final Backup</b> 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.<br>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.<br>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 <b>3G/4G &gt; Data Usage</b> page.  | 160190   |
| Huawei 3G cards do not connect to the Internet after the X1 WAN interface is disconnected.<br>Occurs when one of several Huawei 3G cards is inserted in the TZ appliance and the U0 interface is configured as the <b>Final Backup</b> in the <b>Network &gt; Failover &amp; LB</b> page.   | 159273   |

## Application Control

| Known issue  | Issue ID |
|--|----------|
| The Ultrasurf browser plugin is not blocked by an App Rule or App Control Advanced policy.<br>Occurs when using the Chrome browser plugin for Ultrasurf.   | 161651   |
| 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.<br>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. | 157692   |
| App Control Advanced does not block the Psiphon client version 95 or 87.<br>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.   | 151710   |

## Bandwidth Management

| Known issue   | Issue ID |
|---|----------|
| An Advanced BWM policy works for egress traffic, but not for ingress traffic.<br>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. | 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 |
|--|----------|
| <p>Failover occurs unexpectedly when the aggregator port goes down in a Layer 2 Link Aggregation Group, but the associated member port remains up.</p> <p>Occurs when the High Availability <b>Active/Standby Failover only when ALL aggregate links are down</b> option is enabled and only one port in the L2 LAG is down.</p>                             | 178299   |
| <p>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.</p> <p>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.</p> | 171787   |

## Log

| Known issue  | Issue ID |
|--|----------|
| <p>Cannot modify a syslog server port.</p> <p>Occurs when trying to modify the syslog port from a GMS server.</p>  | 160355   |
| <p>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.</p> <p>Occurs when viewing the App Rules log messages.</p> | 149458   |

## Networking

| Known issue  | Issue ID |
|--|----------|
| <p>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.</p> <p>Occurs when the X-Series switch is set up for <b>Dynamic IP</b>, thus receiving a new IP address when the DHCP server is enabled.</p> <p><b>Workaround:</b> During the initial set up of the X-Series switch, be sure to choose <b>Static IP</b> instead of <b>Dynamic IP</b>.</p> | 170141   |
| <p>Portshielding X-Series switches on a TZ series appliance takes too long.</p> <p>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.</p>  | 170026   |
| <p>The firewall cannot form full adjacency with all neighboring routers using OSPF.</p> <p>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.</p>   | 166564   |
| <p>An IPv6 BGP neighbor cannot be established.</p> <p>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.</p>  | 157525   |
| <p>The firewall cannot enable OSPF through the console.</p> <p>Occurs when trying to enable the OSPF through the firewall console. The network needs to first match the OSPF wildcard bits.</p>  | 153350   |
| <p>The firewall cannot enable RIPv2 through the console.</p> <p>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.</p>   | 153267   |
| <p>The firewall learns OSPF routes from areas other than area0.</p> <p>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.</p>   | 153096   |
| <p>There is no option to originate a default route for dynamic IPv6 routing via OSPFv3.</p> <p>Occurs when configuring OSPFv3 from the <b>Network &gt; Routing</b> page. IPv6 default route origination via OSPFv3 is currently not supported.</p>   | 150771   |

## SSL VPN

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

## Switching

| Known issue   | Issue ID |
|---|----------|
| <p>The aggregated member interface of a Layer 2 Link Aggregation Group (LAG) fails to aggregate into the LAG after restarting the firewall.</p> <p>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.</p> | 167254   |

## System

| Known issue   | Issue ID |
|---|----------|
| <p>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".</p> <p>Occurs when using <b>Send Diagnostic to Support</b> from the <b>System &gt; Settings</b> page.</p> | 163181   |

## User Interface

| Known issue  | Issue ID |
|--|----------|
| <p>Firmware upgrade fails when uploaded through the SonicOS management user interface.</p> <p>Occurs when a firmware upgrade for a Dell X-Series 4012 extended switch is attempted through the SonicOS management interface.</p> <p><b>Workaround:</b> Upgrade the switch firmware directly from the extended switch.</p>  | 171763   |
| <p>The <b>Dashboard &gt; Real-Time Monitor</b> display does not appear to work properly on TZ series appliances with X-Series switches.</p> <p>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 <b>Dashboard &gt; Real-Time Monitor</b> 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 <b>Dashboard &gt; Real-Time Monitor</b> is not applicable.</p> | 169000   |

## VPN

| Known issue  | Issue ID |
|--|----------|
| <p>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.</p> <p>Occurs when <b>IPSEC Management Tunnel</b> is selected as the <b>Management Mode</b> in the GMS settings configured from the <b>System &gt; Administration</b> page on the managed firewall.</p> | 178775   |
| <p>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.</p> <p>Occurs when the configuration settings file on the VPN-bound interface is incompatible with 6.2.x.</p>   | 143210   |

## WAN Acceleration

| Known issue   | Issue ID |
|---|----------|
| <p>In the Tech Support report, the WAN Acceleration module is insufficient to show diagnostics information.</p> <p>Occurs when WAN Acceleration module is not up-to-date so the details about the inner state of this module are not known.</p> | 179852   |

## Wireless

| Known issue   | Issue ID |
|---|----------|
| <p>Clients cannot communicate with each other when they are connected to the firewall using different SonicPoint N endpoints in the same WLAN interface.</p> <p>Occurs when the SonicPoint N endpoints are managed through layer 3 and the Allow Interface Trust option for the WLAN zone is enabled.</p> | 180037   |

# System compatibility

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

## Wireless 3G/4G broadband devices

SonicOS 6.2.5.3 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 6.2.5.3 requires GMS 8.1 service pack 1, which is now available.

## 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

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

**i** **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.

---

Last updated: 11/28/2016

232-003429-00 Rev B