Dell SonicWALL™ SonicOS 6.2.3.1

Release Notes

April 2015

These release notes provide information about the Dell SonicWALL™ SonicOS 6.2.3.1 release.

- About SonicOS 6.2.3.1
- Supported platforms
- Known issues
- System compatibility
- Product licensing
- Technical support resources
- About Dell

About SonicOS 6.2.3.1

SonicOS 6.2.3.1 is a General Release for the new Dell SonicWALL TZ network security appliances. The new TZ300, TZ400, TZ500, and TZ600 firewalls represent the 6th generation of Dell SonicWALL firewalls and provide a major hardware and software upgrade over the previous TZ and NSA 220/250 platforms. The benefits and capabilities of the new TZs include:

- Deep Packet Inspection security without sacrificing performance
- Performance increase based on:
    - Higher processor core speeds
    - Higher processor core count
    - Processor architecture enhancements
    - Additional memory
- 5 to 10 gigabit Ethernet ports, depending on model

TZ feature information

Dell SonicWALL TZ appliances running SonicOS 6.2.3.1 support most of the features provided for other platforms in earlier 6.2 releases. However, some features are not supported on the TZ appliances.

The following features are not supported on the TZ appliances in SonicOS 6.2.3.1:

- Active/Active Clustering
- Advanced Switching
- Jumbo Frames
- Link Aggregation

- Port Redundancy
- Wire Mode
- WXA Clustering

Supported platforms

The SonicOS 6.2.3.1 release is supported on the following Dell SonicWALL network security appliances:

- Dell SonicWALL TZ300
- Dell SonicWALL TZ400
- Dell SonicWALL TZ500
- Dell SonicWALL TZ600

Known issues

The following is a list of known issues in this release.

3G/4G

Known issue	Issue ID
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
Some 3G/4G USB cards are not detected by SonicOS. Occurs when an ATT340U or Sprint 341U card is inserted into the U0 interface on the TZ and the firewall is rebooted one or more times.	159366
Huawei 3G cards do not connect to the Internet after the X1 WAN interface is disconnected. Occurs when one of several the 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

DPI-SSL

Known issue	Issue ID
Applications such as YouTube are slow to load or do not load properly. Occurs when the DPI-SSL service is enabled and policies are configured with Advanced Bandwidth Management; the policies might not work as configured.	158183

Log

Known issue	Issue ID
Alert messages are not displayed in the Latest Alerts section of the System > Status page. Occurs when there are changes to the system which should generate alerts, such as when interfaces are enabled or disabled.	159940

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.	149458
Occurs when viewing the App Rules log messages.	

Networking

Known issue	Issue ID
An IPv6 BGP neighbor cannot be established.	157525
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.	
A Layer 2 Bridge mode interface connection cannot be auto flushed and the connection monitor displays "connection add direction incorrect."	157289
Occurs when interfaces are configured in Layer 2 Bridge Mode and the server responds with a FIN packet for a closed connection.	
The firewall cannot enable OSPF through the console.	153350
Occurs when trying to enable the OSPF through the firewall console. The network needs to first match the OSPF wildcard bits.	
The firewall cannot enable RIPv2 through the console.	153267
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.	
The firewall learns OSPF routes from areas other than area0.	153096
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.	
There is no option to originate a default route for dynamic IPv6 routing via OSPFv3.	150771
Occurs when configuring OSPFv3 from the Network > Routing page. IPv6 default route origination via OSPFv3 is currently not supported.	

SSL VPN

Known issue	Issue ID
Clicking the "here" link on the Virtual Office portal causes the browser to redirect to the https://WANIP:4433/npNLChrome.crx page.	159879
Occurs when using the Chrome browser.	

System

Known issue	Issue ID
The WLAN interface displays "No SonicPoint" after one or more SonicPoints are connected.	159437
Occurs when configuration settings with the SonicPoint Limit set to 24 are imported from a NSA 250M to a TZ500, and then one or more SonicPoints are connected to the WLAN interface on the TZ and it is rebooted.	
Workaround: Sync the SonicPoints to change them all to Operational.	
After importing the configuration settings file from an appliance running 5.9.0.x or 5.9.1.0 to a TZ600 running 6.2.3.1, the interface to which the site-to-site VPN policy is bound changes from X1 to X0.	159034
Occurs when the configuration settings file on the VPN bound interface is incompatible with 6.2.x.	

Known issue	Issue ID
DHCP using IP Helper does not work over a site-to-site VPN. Occurs when one firewall has a DHCP server configured on X0 and is connected on X1 by site-to-site VPN to X1 on a second firewall that has an IP Helper policy configured from X0 to the first firewall's X0 IP address. A client machine connected to the second firewall's X0 cannot obtain an IP address.	159987
The site-to-site VPN tunnel between the appliance and Microsoft Azure sometimes drops and is not automatically renegotiated. Occurs when MS Azure initiates a connection suggesting that both IPv4 and IPv6 "ANY" networks should be protected by the VPN, but on the SonicOS side the VPN configuration is IPv4 based and the mixed IPv4/IPv6 configuration cannot be validated and processed. If the connection is initiated by the SonicWALL appliance, it only suggests that the IPv4 "ANY" network should be protected by the VPN, which is accepted by the MS Azure gateway and the VPN tunnel works as expected. **Workaround**: If the VPN tunnel is down, the SonicOS administrator can initiate the connection from the SonicWALL appliance by disabling, then re-enabling the tunnel.	157568
Unable to establish connectivity to Amazon VPC using Dynamic Routing BGP. Occurs when using VPN Numbered Tunnel Interfaces with VPNs whose names are longer than 16 characters.	156859

System compatibility

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

Wireless 3G/4G broadband devices

SonicOS 6.2.3.1 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/us/en/products/3190.html.

GMS support

Dell SonicWALL Global Management System (GMS) 7.2 Service Pack 4 is required for GMS management of Dell SonicWALL TZ300, TZ400, TZ500, and TZ600 security appliances running SonicOS 6.2.3.1.

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 6.2.3.1. The recommended firmware version for the WXA series appliances is WXA 1.3.1.

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.

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

- Chat with a support engineer

- 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 www.software.dell.com.

Contacting Dell

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

Patents

For more information about applicable patents, refer to http://software.dell.com/legal/patents.aspx.

Trademarks

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

_____