Dell SonicWALL™ SonicOS 6.2.4.2

Release Notes

August 2015, revised December 2015

These release notes provide information about the Dell SonicWALL™ SonicOS 6.2.4.2 release.

About SonicOS 6.2.4.2

SonicOS 6.2.4.2 is the initial webpost release for the Dell SonicWALL SOHO Wireless, and is a maintenance release for Dell SonicWALL TZ and TZ Wireless series network security appliances.

NOTE: SonicOS 6.2.4.x does not support unnumbered tunnel interfaces. Numbered tunnel interfaces are supported on all platforms and can be configured and used in the same way as standard interfaces. However, this design change can cause issues when upgrading an appliance from SonicOS 6.2.3.1 to 6.2.4.x. For more information, see the **VPN** table in the Known issues section. For a 6.2.4-based Hotfix firmware supporting unnumbered tunnel interfaces, contact Support at: https://support.software.dell.com/manage-service-request.

TZ Series/SOHO Wireless feature support

Dell SonicWALL SOHO Wireless and TZ series appliances running SonicOS 6.2.4.2 support most of the features available for other platforms in earlier 6.2 releases. 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

Supported platforms

The SonicOS 6.2.4.2 release is supported on the following Dell SonicWALL network security appliances:

- SOHO Wireless
- TZ300 and TZ300 Wireless
- TZ400 and TZ400 Wireless
- TZ500 and TZ500 Wireless
- TZ600

Resolved issues

This section contains a list of issues that are fixed in this release.

3G/4G

Resolved issue	Issue ID
The Verizon 551L 4G USB device is not recognized and does not connect. Occurs when the device is plugged into a SOHO Wireless appliance.	163683

Log

Resolved issue	Issue ID
Creating an FQDN Address Object while adding a syslog server results in an error message, “Error: Aux Syslog Server Address: Syslog Server Address.: validation failed; check value”. Occurs when attempting to use a name such as “www.1b.com” for the FQDN Address Object while adding a syslog server.	163516

Networking

Resolved issue	Issue ID
A NAT policy priority cannot be set to zero, which applies automatic priority settings. Occurs when the priority of the NAT policy was previously manually changed to the same priority as another NAT policy, causing the two NAT policies to swap priorities.	163823
A NAT policy cannot be edited, but gives the error message, “policy's IP version can't be edited”. Occurs when an IPv6 NAT policy for the CU-SeeMe service is created and then the administrator attempts to edit the policy.	163155
A VLAN interface uses an old default MAC address and cannot connect to the PPPoE server. Occurs when the VLAN interface is configured in WAN PPPoE mode and is connected to the PPPoE server, and then the Override Default MAC Address option is enabled on the parent (physical) interface and the VLAN interface is disconnected and tries to reconnect to the PPPoE server.	162586
There is no way to force specific link speed/duplex on the TZ400/TZ500 X1 interface. Occurs when configuring the X1 interface on the Network > Interfaces page to work with a switch or other hardware that does not support auto-negotiation of the link speed and duplex.	159144

SSL VPN

Resolved issue	Issue ID
An Any-to-Any Allow All firewall access rule is not automatically added for SSLVPN to SSLVPN. Occurs when configuring the SSLVPN zone on the Network > Zones page and selecting the Allow Interface Trust checkbox, then clicking OK.	162894

System

Resolved issue	Issue ID
The 'Last' and 'All' trace logs are empty. Occurs when these log files contain messages and then the firewall is restarted without removing power (a soft or warm reboot). This is fixed as follows: • The 'Last' trace logs will continue to be empty. • The 'Current' logs are now preserved across reboots (not power-cycles) and contain information about the reboot cause and earlier system events. • Critical messages are logged in a wrapping buffer.	161201

User Interface

Resolved issue	Issue ID
A wireless guest user cannot connect to the Internet and a JavaScript error is displayed in the SonicOS management interface. Occurs when WiFiSec enforcement is enabled and a guest account is created and the Enable Wireless Guest Services checkbox is selected in Network > Zones for the WLAN zone, and then a wireless guest user connects to the SSID and attempts to access the Internet.	163101

VPN

Resolved issue	Issue ID
NAT policies automatically created during L2TP configuration are not removed as expected. Occurs when an L2TP server is enabled and a DNS server and L2TP IP address pool are configured, causing several NAT policies to be automatically created, and then the L2TP server is disabled.	163582

Wireless

Resolved issue	Issue ID
Changing the Virtual Access Point SSID appears to work, but the previous SSID remains available to wireless clients and the new SSID is not. Occurs when the VAP SSID is changed in an internal AP group while a client is still connected. The Wireless > Settings page shows the new SSID. Then the client is disconnected, its wireless interface is disabled and enabled again, and then it searches for a wireless SSID and can connect to the old one but does not see the new one at all.	163154
After connecting a wireless bridge to a WPA2/WPA access point successfully in wireless bridge mode, it cannot connect to an access point with WEP or Open AP, and link status shows "Disconnected". Occurs when the mode is changed from WPA to Open/WEP.	161725

Known issues

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

3G/4G

Known issue	Issue ID
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
3G/4G cards are not detected as the firewall starts up. Occurs when a 3G or 4G card is inserted into a TZ wireless or SOHO wireless firewall while it is powered down, and then the firewall is started up. **Workaround**: Pull the card out and then plug it back in while the firewall remains up. Or, restart the firewall without the 3G/4G card, and insert the card into the firewall after it comes up.	160638
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 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
App Control Advanced does not block the Psiphon client version 95 or 87. 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.	162055
The Ultrasurf browser plugin is not blocked by an App Rule or App Control Advanced. 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. 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

DPI-SSL

Known issue	Issue ID
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. 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.	163672
The Google Drive application cannot connect and synchronize data with Google servers, but fails due to an unknown CA certificate. Other applications also have this issue. Occurs when DPI-SSL is enabled on the firewall when using Google Drive, Apple iTunes, or any other application with pinned certificates. **Workaround**: Exclude the associated domains from DPI-SSL, such as excluding the following to allow Google Drive to work: • .google.com • .googleapis.com • .gstatic.com Since Google uses one certificate for all its applications, this allows all Google applications to bypass DPI-SSL. Alternatively, exclude the client machines from DPI-SSL.	162719
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
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
LAN to WAN traffic through a VLAN sub-interface fails with the message "Destination MAC address is not our interface". Occurs when the X1 WAN interface is configured in PPPoE mode and the Override Default MAC Address option is enabled on X1, then a VLAN sub-interface is bound to X1 and also configured in PPPoE mode. After both X1 and the VLAN interface connect to the PPPoE server, traffic from the Internet to the VLAN IP address is dropped. Diagnostics show that the MAC address for the VLAN interface is the original rather than the override address.	163733
The DHCP Server lease scope assigned to X0 is changed to belong to X3. Occurs when DHCP Server is initially enabled on X0 and the administrator attempts to configure X3 in Layer 2 Bridged mode, bridged to X0, but receives an error that the DHCP Server is enabled on the primary interface. After disabling DHCP Server on X0, X3 is successfully bridged to X0 and then the Network > DHCP Server page displays the previous X0 DHCP Lease Scope as now belonging to X3.	163199
Advanced routing does not work on both a parent interface and VLAN sub-interface at the same time. OSPF stays in NULL status and RIP cannot learn any routes. Occurs when OSPF and RIP are enabled on a parent physical interface and on a VLAN sub-interface such as on X4 and X4:v140.	163188

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
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

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
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. Occurs when the configuration settings file on the VPN bound interface is incompatible with 6.2.x.	143210

Upgrading

Known issue	Issue ID
Automatically added access rules for a VPN tunnel policy do not work after upgrading the appliance and traffic can no longer pass between clients on either side of the tunnel. Occurs when a VPN tunnel policy is added and bound to X1 on this firewall and the same on another firewall, then a route policy is manually added on this firewall with destination set to the LAN subnet of the other firewall, using the VPN tunnel policy as the interface. Access rules are automatically added on both firewalls for LAN > VPN and VPN > LAN, and traffic can pass between clients connected to each firewall. The first firewall is then upgraded from 6.2.3.1 to 6.2.4.1, causing the manually added route policy to be removed, but the access rules remain.	163388

User Interface

Known issue	Issue ID
A JavaScript error prevents manual key configuration. Occurs when attempting to configure an IPv6 manual key policy.	163802

Users

Known issue	Issue ID
The login redirect page fails to display and no websites can be accessed from a client computer on the LAN. Occurs when the User authentication method is set to LDAP or RADIUS, the default user group is configured as Everyone, and the access rules for LAN>WAN allow the user group Everyone.	164220
The Test LDAP User function returns 'LDAP communication error'. Occurs when Local User is configured for the User authentication method and an LDAP server is correctly configured.	162500

VPN

Known issue	Issue ID
Unnumbered tunnel interfaces are not displayed in the Interface drop-down list in the Add Route Policy window. After upgrading from 6.2.3.1 to 6.2.4.x: • All unnumbered tunnel interfaces created in SonicOS 6.2.3.1 with routing policies are changed to *unknown* and traffic cannot be routed through the interfaces. • The auto-added access rules for VPN connections that used unnumbered tunnel interfaces still exist and cannot be deleted. Occurs when an appliance is running SonicOS 6.2.4.x or when it is upgraded from SonicOS 6.2.3.1 to 6.2.4.x. This is due to a design change in which *numbered* tunnel interfaces can be supported on all platforms including those with memory constraints, leading to removal of support for unnumbered tunnel interfaces.	160360, 160438, 160578
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

System compatibility

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

Wireless 3G/4G broadband devices

SonicOS 6.2.4.2 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/us/en/products/3190.html.

GMS support

Dell SonicWALL Global Management System (GMS) 7.2 Service Pack 5 or GMS 8.0 HotFix 161632 is required for GMS management of Dell SonicWALL SOHO Wireless, TZ300 Wireless, TZ400 Wireless, and TZ500 Wireless security appliances running SonicOS 6.2.4.2.

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 6.2.4.2. 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.

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

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Patents

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

Trademarks

Dell, the Dell logo, and SonicWALL are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

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.

Last updated: 12/2/2015

232-002988-00 Rev B