Dell SonicWALL™ SonicOS 5.9.1.3

Release Notes

April 2015

These release notes provide information about the Dell SonicWALL™ SonicOS 5.9.1.3 release.

- About SonicOS 5.9.1.3
- Supported platforms
- Known issues
- System compatibility
- Product licensing
- Technical support resources
- About Dell

About SonicOS 5.9.1.3

SonicOS 5.9.1.3 is the Initial Release for the Dell SonicWALL SOHO network security appliance.

The Dell SonicWALL SOHO represents the 6th generation of SonicWALL firewalls and provides a hardware and software upgrade over the previous SonicWALL TZ 105 platform. The SonicWALL SOHO provides Deep Packet Inspection security without sacrificing performance, higher performance overall, and a platform with 5 ports, all gigabit Ethernet.

SOHO feature information

Dell SonicWALL SOHO appliances running SonicOS 5.9.1.3 support most of the features provided for other platforms in earlier 5.9 releases. However, the following features are not supported on the SonicWALL SOHO:

- Active/Active Clustering
- AppFlow Reports
- BGP Advanced Routing
- Numbered Tunnel Interfaces for Route Based VPN
- Single Sign-On RADIUS Accounting
- SonicPoint Layer 3 Management
- Wire Mode

Supported platforms

The SonicOS 5.9.1.3 release is supported on:

- Dell SonicWALL SOHO

Known issues

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

Command line interface

Known issue	Issue ID
The command "show sonicpoint all-discovered-access-points" results in an error message and does not display the list of SonicPoints. Occurs when the command is entered on the command line.	158939

IPv6

Known issue	Issue ID
A 6rd tunnel (IPv6 rapid deployment tunnel) is unexpectedly reported as UP although there is no available 6rd prefix. Occurs when the tunnel was previously UP and using DHCP mode, and then the DHCP server is disabled and the firewall is rebooted.	157034

Log

Known issue	Issue ID
Some log entries display the characters "%s" in the alert message instead of displaying the specific alert information. Occurs when logging alerts from Application Firewall, which appear as "Application Firewall Alert %s".	159279

Networking

Known issue	Issue ID
Changing the X1 interface from PPTP mode to static mode causes X1 to become inaccessible and changes its IP address to 0.0.0.0. Occurs when the X1 interface has obtained an IP address in PPTP mode and then the administrator reconfigures X1 in static mode and gives it a static IP address. **Workaround**: Restart the firewall to make X1 accessible again.	160164
An automatically created group address object becomes editable on the Network > Address Objects page and attempting to delete it causes an error message, "Error: Object is in use by an Access Rule" although it is not referenced by any ACL. Occurs when a group address object called "*<custom zone name>* Interface IPv6 Addresses" is created by the system after adding a custom zone in Network > Zones, and then the custom zone is deleted.	156481

The default route gateway is wrong after changing the WAN mode.	154144
Occurs when X1 is configured with IP Assignment in L2TP mode, then changed to PPTP mode, but the default route gateway is still the one learned from the L2TP server. After changing the WAN mode back to L2TP, the default route gateway is the one learned from the PPTP server.	
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.	

System

Known issue	Issue ID
The error message, "Error: Attempt to upgrade to an invalid product code!!Active Product Code was 12800" is displayed.	157287
Occurs when the firewall is running the debug firmware and is rebooted. No error message is seen when running production firmware (non-debug).	

User interface

Known issue	Issue ID
The hyperlink in "Click here for UTM management" does not work.	157523
Occurs when logged into the IPv6 address of the SSL VPN Virtual Office portal.	

System compatibility

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

Dell SonicWALL WXA support

The Dell SonicWALL WXA series appliances and software deployments (WXA 6000 Software, WXA 500 Software, WXA 5000 Virtual Appliance, WXA 2000/4000 appliances) are supported for use with Dell SonicWALL security appliances running SonicOS 5.9. The recommended software/firmware version for the WXA series is WXA 1.3.1.

GMS support

Dell SonicWALL Global Management System (GMS) 7.2 Service Pack 4 is required for GMS management of Dell SonicWALL SOHO appliances running SonicOS 5.9.1.3.

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 8.0 and higher (do not use compatibility mode)

- Safari 5.0 and higher

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, go 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: 4/28/2015

232-002855-00 Rev A