Dell SonicWALL™ SonicOS 5.9.1.0

Release Notes

December, 2014

These release notes provide information about the Dell SonicWALL SonicOS 5.9.1.0 release.

About SonicOS 5.9.1.0

SonicOS 5.9.1.0 introduces support for the Dell SonicPoint ACe, ACi, and N2 wireless access points on Dell SonicWALL network security appliances capable of running SonicOS 5.9 firmware.

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 5.9.0.x. For more information, see the previous release notes:

SonicOS 5.9.0.7 Release Notes	https://support.software.dell.com/download/downloads?id=5744033
SonicOS 5.9.0.6 Release Notes	https://support.software.dell.com/download/downloads?id=5556192
SonicOS 5.9.0.4 Release Notes	https://support.software.dell.com/download/downloads?id=5480524
SonicOS 5.9.0.2 Release Notes	https://support.software.dell.com/download/downloads?id=5371337
SonicOS 5.9.0.1 Release Notes	https://support.software.dell.com/download/downloads?id=5371336
SonicOS 5.9.0.0 Release Notes	https://support.software.dell.com/download/downloads?id=5371335

Supported platforms

The SonicOS 5.9.1.0 release is supported on the following Dell SonicWALL network security appliances:

• NSA E8510	• NSA 2400	• TZ 215	• TZ 215 Wireless
• NSA E8500	• NSA 2400MX	• TZ 210	• TZ 210 Wireless
• NSA E7500	• NSA 250M	• TZ 205	• TZ 205 Wireless
• NSA E6500	• NSA 250M Wireless	• TZ 200	• TZ 200 Wireless
• NSA E5500	• NSA 240	• TZ 105	• TZ 105 Wireless
• NSA 5000	• NSA 220	• TZ 100	• TZ 100 Wireless
• NSA 4500	• NSA 220 Wireless		
• NSA 3500			

New features

SonicOS 5.9.1.0 provides support for the new Dell SonicPoint wireless access points:

- Dell SonicPoint ACe — 802.11ac compliant with external antennas
- Dell SonicPoint ACi — 802.11ac compliant with internal antennas
- Dell SonicPoint N2 — 802.11n compliant with external antennas

Dell SonicPoint ACe and ACi support the 802.11ac standard for Wi-Fi. This includes higher throughput in the 5-GHz band, wider channels, more spatial streams, and other features that boost throughput and reliability. The Dell SonicPoint ACe/ACi provide the following key technical components:

- Wider Channels—80 MHz channel bandwidths
- New Modulation and Coding—64-QAM, rates 3/4 and 5/6 added as option modes
- Up to 4 Spatial Streams—Adding spatial streams increases throughput proportionally. Two streams doubles the throughput of a single stream. Four streams increases the throughput four times.

Dell SonicPoint ACe, ACi, and N2 provide dual radios for wireless access on both the 5-GHz and 2.4-GHz radio bands.

Dell SonicPoint ACi and N2 are powered by 802.3at compliant Power Over Ethernet (PoE).

Dell SonicPoint ACe can be powered by 802.3at compliant PoE or with the included power adaptor (input 120V-240V AC to output 12V DC).

Resolved issues

The following issues are resolved in this release.

Anti-Spam

Resolved issue	Issue ID
Anti-Spam cannot be re-enabled and the error message “Mail Server Auto-Detect Failed” is displayed. Occurs when Anti-Spam is successfully enabled, and then the administrator disables it by clearing the "Enable Anti-Spam Service" checkbox and accepting the changes, and then selects the checkbox to enable Anti-Spam again.	140099

Log

Resolved issue	Issue ID
The Log Monitor page stops responding and displays “Processing Please wait...”. Occurs when VPN names include the pipe character "|", which is also used for the table format in the Log Monitor page.	153449

Networking

Resolved issue	Issue ID
Traffic from a client computer to the Internet incorrectly uses the default route. Occurs when the computer’s gateway is not set to the Layer 2 Bridge interface.	154747
Dynamic DNS displays “Network error”. Occurs when the online mode is changed to "Let the DDNS provider detect the IP Address".	145082
The Restore Defaults button on the Firewall > Access Rules page does not always restore the default rules. Occurs when a default access rule is modified, such as the default LAN > WAN rule.	135296

Users

Resolved issue	Issue ID
A WAN to LAN access rule initially blocks access for unauthorized users, but then allows access. Occurs when a Web server is set up behind the firewall and a WAN > LAN access rule only allows access to users authenticated on RADIUS, and then a non-RADIUS user connects over HTTPS from an external location.	151249

Wireless

Resolved issue	Issue ID
The BSSIDs are not unique for Virtual Access Points (VAPs) configured for a SonicPoint. Occurs when using a SonicPoint AC with dual radios. Each radio supports 8 VAPs.	154770
A wireless client cannot connect to a SonicPoint AC or N2 access point. Occurs when the authentication method is WEP with Remote Address Access control enabled.	154183
The Wireless > Settings page does not display the list of internal channels. Occurs when using a Dell SonicWALL TZ 200W.	154140

Resolved issue	Issue ID
There is no UI response after clicking the OK button after trying to add a VAP profile, and a JavaScript error is displayed, “Uncaught TypeError: Cannot read property 'value' of undefined”. Occurs when trying to add a VAP profile with the “Enable Remote MAC Access Control” option selected.	151552

Wizards

Resolved issue	Issue ID
The Setup Wizard cannot complete the initial setup configuration and the firewall must be restarted. The Setup Wizard stops on the WAN Settings page after the "Next" button is clicked, and displays an error message. Occurs when trying to configure the initial settings using the Setup Wizard.	135211

Known issues

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

3G/4G

Known issue	Issue ID
The appliance does not redial to re-establish the 4G WAN connection after a few successful redials on lost connections overnight. Occurs when using the Verizon Pantech UML290VW or AT&T Momentum with a firewall. Observed on TZ 105, 200, or 200W appliances. **Workaround**: Reboot the appliance.	150123
The 3G/4G device is connected, but no traffic passes through it. Occurs when interface U0 is configured as the final backup or as the primary WAN, and the Wireless 3G/4G device is connected without an external antenna. Thus, it is only able to negotiate HSPA+. Traffic when using an external antenna to negotiate with the faster LTE network.	133999
The firewall shuts down or restarts automatically when a 3G/4G USB device is inserted or removed. Occurs when inserting or removing a 3G/4G USB device when the appliance is powered on. **Workaround**: The appliance should always be powered off when inserting or removing a USB device. Hot plug and play is not supported.	130973

Active/Active Clustering

Known issue	Issue ID
The backup units do not synchronize with the updated configuration on the active units. Occurs when all connection ports on both backup units are disconnected, and the CLI is used to configure X0 on the active unit, to enable the “RIP” and “Send Only” options. Then, the backup units are reconnected.	130316
No Virtual Group selection is available when using the Public Server Rule wizard on an Active/Active Clustering pair. The new policy is bound to Group 1. Occurs when configuring a NAT policy and adding a public server for Group 2 from the Public Server Rule wizard. **Workaround**: Manually edit the NAT policy after using the wizard.	128631

Application Control

Known issue	Issue ID
An application is blocked by the firewall even though the client IP address is in the "excluded IP address range" list. Occurs when App Control is enabled and excluded traffic is sent through the firewall.	139176
The App Rule Match Object cannot match a filename. Occurs during an FTP download or upload and the Match Type of the Firewall > Match Object is set to Prefix Match, the Input Representation is set to Hexadecimal Representation, and the Enable Negative Matching option is selected. **Workaround**: Do not enable the Negative Matching option with the Prefix Match option.	135634
Known issue	**Issue ID**
App Control policies do not block IPv6 traffic unless Intrusion Prevention Service (IPS) is enabled. Occurs when IPS is disabled and an App Control policy is created from Firewall > App Control Advanced to block FTP traffic. A computer on the LAN side can still use an IPv6 IP address to connect to an FTP server. **Workaround**: Enable IPS. With IPS enabled, the App Control policy blocks the FTP connection.	128410

CLI

Known issue	Issue ID
Access Rules are not removed on the Backup device of an HA pair and further configuration is not synchronized with the Backup device. Occurs when the access-rule restore-defaults CLI command is issued.	141949

DPI-SSL

Known issue	Issue ID
The certificate from a secure website, such as https://mail.google.com, is not changed to a Dell SonicWALL DPI-SSL certificate as it should be, and traffic cannot be inspected. Occurs when the "Enable SSL Client Inspection" option is set on the DPI-SSL > Client SSL page, a SonicPoint-NDR is connected to the appliance, Guest Services are enabled on the WLAN zone, a wireless client connects to the SonicPoint, and the user logs into the guest account.	123097

IPv6

Known issue	Issue ID
IPv6 traffic that is sent over a 6rd interface is not forwarded. Occurs after rebooting the firewall. **Workaround:** Go to the Network > Interfaces page and open the Edit Interface dialog for the 6rd interface and click OK without making any changes. Traffic should be forwarded after that.	143079
IPv6 packets exceeding the Maximum Transmission Unit (MTU) are dropped instead of being fragmented. Occurs when setting the MTU for an interface, and then sending IPv6 packets that exceed the MTU.	139108
An IPv6 Address Object in the Exclusion Address list of an App Rule policy is still blocked by that App Rule policy. Occurs when a computer on the LAN with an IPv6 address that is in the Exclusion Address list of an App Rule policy tries to connect to an IPv6 website that is blocked by that policy.	128363

Log

Known issue	Issue ID
Log settings cannot be modified. The error message, “The format of the email address is incorrectly reported” is displayed. Occurs when trying to modify the log settings in the Edit Log Category dialog on the Log > Settings page.	131932

Networking

Known issue	Issue ID
SonicOS strips the VLAN tag when sending out the return/egress packets. Occurs when VLAN traffic passes through a Layer 2 Bridged interface pair. The traffic arrives tagged with a VLAN number and is forwarded with the correct VLAN tag. The return traffic (echo reply) arrives also tagged with the VLAN number, but the VLAN tag is removed when SonicOS forwards the traffic out the VLAN interface.	154524
VLAN traffic replies are sent out from an unexpected interface. Occurs when a Layer 2 Bridged interface pair is configured, and a VLAN configured on the primary interface of the L2B pair. When a client computer on the VLAN subnet connects to that primary interface and pings the VLAN interface, the reply is sent from the secondary L2B interface and ARP shows the client located on the secondary interface.	154252
Importing settings from SonicOS 5.8 to 5.9 on some platforms eliminates all OSPF and RIP configurations created over VPN tunnel interfaces. After upgrading to 5.9 and importing the 5.8 settings, the VPN tunnel interfaces used for OSPF and RIP are missing. Occurs when SonicOS does not automatically convert unnumbered tunnel interface configurations to numbered tunnel interface configurations. Numbered and unnumbered tunnel interface implementations are mutually exclusive in SonicOS 5.9.x.x, so if numbered tunnel interfaces are supported on a device, unnumbered tunnel interfaces are NOT supported on that device and vice versa.	154120

Numbered Tunnel Interfaces Supported	Unnumbered Tunnel Interfaces Supported	No Tunnel Interfaces Supported
NSA E8510	NSA 2400MX	TZ 200/200W
NSA E8500	TZ 210/210W	TZ 100/100W
NSA E7500	TZ 205/205W	
NSA E6500	TZ 105/105W	
NSA E5500		
NSA 5000		
NSA 4500		
NSA 3500		
NSA 2400		
NSA 250M/250MW		
NSA 240		
NSA 220/220W		
TZ 215/215W		

Workaround: Manually reconfigure VPN tunnel interfaces and routing settings in SonicOS 5.9 after importing settings from SonicOS 5.8.

Known issue	Issue ID
The paired interface does not go down when the other interface in the Wire Mode pair is brought down. Occurs when the "Enable Link State Propagation" option is enabled and a wire mode interface is brought down by performing a shutdown on the peer switch.	151827
Disabling one DHCPv6 client also disables another DHCPv6 client. Occurs when both X1 and X2 are configured to DHCPv6 automatic mode, and then X1 is changed to static mode.	147542
Packets cannot pass through the Wire mode pair. Occurs when the destination link-local IPv6 address is the same as the Wire mode interface address.	144385
The default gateway cannot be configured. Occurs when X2 is configured as a WAN interface and the IP assignment is set to static.	141973
IPv6 NAT policies are not removed from the firewall as expected. Occurs when all the IPV6 custom policies have been deleted and the firewall is restarted.	141530
The Gateway Anti-Virus (GAV) may not work in IPv6 Wiremode > Secure mode. Occurs when using Wiremode > Secure mode with GAV enabled globally and per zone.	139250
Border Gateway Protocol (BGP) authentication does not work with IPv6 peers. Occurs when configuring an IPv6 peer between a firewall and a router, then enabling BGP authentication on each side.	138888
The value of the “ifHCInBroadcastPkts” field in an SNMP-GET packet is different from the value displayed for Rx Broadcast Packets on the Network > Interfaces page. Occurs when comparing the Rx Broadcast Packet values for each interface shown on the Network > Interfaces page with the values obtained from SNMP.	131306

Security Services

Known issue	Issue ID
SonicOS drops the Client CFS Ping reply packets, and Client CFS Enforcement does not work on the SSL VPN zone. Occurs when the source IP address of the Client CFS Ping packet is the WAN interface IP address.	135585
The Gateway AV Exclusion List does not prevent some IP addresses from being blocked. Occurs when an FQDN Address Object is included in the Gateway AV Exclusion List.	121984

SSL VPN

Known issue	Issue ID
SonicOS Web management and SSH management over SSL VPN do not work. Occurs when SonicOS is configured to allow management over SSL VPN and a local user with SSL VPN service and administrator privileges tries to access the X0 subnet, but NetExtender attempts to connect to the default LAN IP address.	153399

System

Known issue	Issue ID
A Web browser is automatically redirected the X1 WAN IP address of the SonicOS appliance instead of the X0 LAN IP address. Occurs after a firmware upgrade when logging into the SonicOS appliance from the LAN zone.	140351
The configuration mode on the LCD panel cannot be accessed and displays an Invalid Code error message. Occurs when the administrator selects the Configuration option on the LCD panel and enters the new PIN code that was just changed on the System > Administration page.	130379
Dell SonicWALL GMS does not synchronize with SonicOS after making password changes in One Touch Configuration and then rebooting the appliance. Occurs when password complexity is changed via One Touch Configuration from GMS. The One Touch Configuration options for Stateful Firewall Security require passwords containing alphabetic, numeric and symbolic characters. If the appliance has a simple password, such as the default “password”, GMS cannot log in after the restart, and cannot be prompted to change the password.	124998
The management computer cannot manage the firewall because SonicOS cannot forward Ethernet packets larger than 1496 KB. Occurs when the management computer is connected to an H3C 10GE switch which is connected in Trunk mode to a second switch and then connected to the firewall 10GE interface.	121657

Users

Known issue	Issue ID
Single Sign-On (SSO) does not work for users behind a proxy server. Occurs when SSO tries to authenticate users behind a proxy server from the “X-Forwarded-For HTTP” header. Two local IP addresses are being saved in the cache: the initiator IP address and the user IP address. Normally these should be the same IP address, but they are not because the user is behind a proxy server and the initiator IP address is that of the proxy server.	135558
Single Sign-On (SSO) only works on Active-Active Clustering Virtual Group 1. SSO does not work on other Virtual Groups. Occurs when SSO agents are configured in a clustered environment. Virtual Group 1 has a green status. However, all other Virtual Groups have a red status and do not work with the SSO Agent.	120202

Known issue	Issue ID
Single Sign-On (SSO) does not work when Guest Services is enabled. Occurs when both SSO and Guest Services are enabled. Guest Services blocks SSO authentication.	119001

VoIP

Known issue	Issue ID
SonicOS drops SIP packets from the WAN to a Layer 2 Bridged LAN interface, and cannot establish a VoIP call. Ping works across the same path. The call can be established when using the primary LAN interface. Occurs when interface X5 (LAN) is configured in L2 bridge mode and bridged to X0 (LAN). A Cisco phone is connected to X5 and is used to make a call to a phone on the WAN side, but the call cannot be established.	128225

VPN

Known issue	Issue ID
VPN negotiation fails and the log for the Initiator does not have an entry showing "IKEv2 negotiation complete". Occurs when the VPN policy is bound to an interface other than the interface for the default route. Observed when the VPN policy is bound to an IPv6 address on both ends.	148167
Traffic goes to the wrong VPN tunnel. Occurs when two VPN tunnel interfaces are configured with Amazon VPC, and we add two numbered tunnel interfaces and BGP neighbors based on the Amazon VPC configuration. When Tunnel 1 goes down, the traffic switches to Tunnel 2. When Tunnel 1 comes back up, the traffic stays on Tunnel 2. When Tunnel 2 goes down, the traffic switches to Tunnel 1. But when Tunnel 2 comes back up, the traffic stops. The route table shows that packets are going through Tunnel 1, but a packet capture shows that packets are going through Tunnel 2.	135205
An active IPv6 VPN tunnel is not displayed in the table on the VPN > Settings screen of the head-end firewall. Occurs when two IPv6 VPN tunnels are created on both the head-end appliance and a remote appliance. The head-end VPN > Settings screen shows “2 Currently Active IPv6 Tunnels”, but it only displays one tunnel in the Currently Active VPN Tunnels table.	128633
An OSPF connection cannot be established between an NSA 240 and an NSA 7500. Occurs when a VPN tunnel is configured between an NSA 240 and an NSA 7500, with Advanced Routing enabled on the NSA 240. A numbered tunnel interface is created on the NSA 7500 and is bound to the VPN tunnel. A VLAN is created on the NSA 240 with an IP address in the same subnet as the Tunnel Interface on the NSA 7500. OSPF is enabled on both appliances, but the NSA 240 does not respond to the OSPF “Hello” packet, and an OSPF connection cannot be established.	128419
The administrator cannot change the Manual Key VPN policy. The following message appears, "Remote IKE ID must be specified." Occurs when the administrator attempts to change a Manual Key VPN policy to an IKE policy. **Workaround:** Delete the Manual Key policy and add a new IKE policy with the same IPsec gateway and source/destination networks.	112988

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 (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are also supported for use with Dell SonicWALL security appliances running SonicOS 5.9. The recommended firmware version for the WXA series appliances is WXA 1.3.0.

WWAN 3G/4G support

SonicOS 5.9 supports a variety of 3G and 4G PC cards and USB devices for Wireless WAN connectivity. To use a 3G/4G interface you must have a 3G/4G PC card and a contract with a wireless service provider. A 3G/4G service provider should be selected based primarily on the availability of supported hardware, which is listed at: http://www.sonicwall.com/us/products/cardsupport.html.

In addition to devices supported on previous releases, SonicOS 5.9 includes support for the following 3G/4G devices:

- "T-Mobile Rocket 3.0" ZTE MF683 4G (USA)
- "AT&T Momentum" Sierra Wireless 313U 4G (USA)
- "AT&T Beam AirCard" Sierra Wireless 340U 4G (USA) (supported with LTE network, not with HSPA+)
- Pantech UML290 4G (USA)
- "Rogers Rocket Stick" Sierra Wireless 330U 4G (Canada)
- Huawei E398
- Huawei E353
- Kyocera 5005 (Vodafone's branded implementation of the Huawei E398)

NOTE: When connected to a Dell SonicWALL appliance, the performance and data throughput of most 3G/4G devices will be lower than when the device is connected directly to a personal computer. SonicOS uses the PPP interface rather than the proprietary interface for these devices. The performance is comparable to that from a Linux machine or other 4G routers.

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.

After your Dell SonicPoint ACi, ACi, or N2 is connected to a registered Dell SonicWALL network security appliance, SonicOS will automatically register the SonicPoint on MySonicWALL, if connected to the Internet. It may take up to 24 hours for your SonicPoint to be automatically registered. Optionally, you can manually register your SonicPoint on MySonicWALL by logging into your account at: http://www.mysonicwall.com.

All Dell SonicPoint wireless access points include an initial subscription to Dell SonicWALL 24x7 Support. In order to receive technical support, your SonicPoint must have an active Support subscription.

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 5.9 Upgrade Guide*, available on MySonicWALL or on the Dell Software Support page for SonicWALL NSA or TZ series appliances:

https://support.software.dell.com/download/downloads?id=5371313

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. To access the Support Portal, go to http://software.dell.com/support/.

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

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.

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

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: 12/20/2014

232-002761-00 Rev A