Dell SonicWALL™ SonicOS 5.9.1.1

Release Notes

June, 2015

These release notes provide information about the Dell SonicWALL SonicOS 5.9.1.1 release.

About SonicOS 5.9.1.1

SonicOS 5.9.1.1 is a maintenance release that fixes a number of issues found in previous releases. See Resolved issues. It also provides enhancements for supporting international Dell SonicPoint wireless access points and vulnerability prevention. See Enhancements.

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 5.9.0.x and 5.9.1.x. For more information, see the release notes for these releases, available at https://support.software.dell.com/release-notes-product-select:

- SonicOS 5.9.1.0
- SonicOS 5.9.0.7
- SonicOS 5.9.0.6
- SonicOS 5.9.0.4
- SonicOS 5.9.0.2
- SonicOS 5.9.0.1
- SonicOS 5.9.0.0

Supported platforms

The SonicOS 5.9.1.1 release is supported on the following Dell SonicWALL network security appliances:

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

Enhancements

- Dell SonicPoint support for Japan
- International Dell SonicPoint support
- Resolved vulnerabilities

Dell SonicPoint support for Japan

SonicOS 5.9.1.1 supports Dell SonicPoint ACe, ACi, and N2 wireless access points for deployment in Japan.

International Dell SonicPoint support

SonicOS 5.9.1.1 supports international Dell SonicPoint ACe, ACi, and N2 wireless access points. An international SonicPoint is one that is deployed and operating in a country other than the United States or Japan.

When an international Dell SonicPoint is connected to a Dell SonicWALL network security appliance, SonicOS displays a **Register** button on the SonicPoint > SonicPoints page. Clicking **Register** brings up a dialog box in which you can select the appropriate **Country Code**.

> ⓘ **NOTE:** Be sure to select the country code for the country in which the Dell SonicPoint will be deployed, even if you are not in that country while registering the SonicPoint.

For international SonicPoints registered with country codes other than Canada, the country code can be changed in the SonicPoint profile on the SonicPoint > SonicPoints page.

> ⓘ **IMPORTANT:** Once the SonicPoint is registered with the country code for Canada, the country code cannot be changed except by contacting Dell SonicWALL Support.

Resolved vulnerabilities

The following potential vulnerabilities are fixed in this release:

- CVE-2014-0198 – Denial of Service vulnerability
- CVE-2010-5298 – Data injection and Denial of Service vulnerability
- VL-ID 1359 – Client Side Cross Site Scripting vulnerability
- OpenSSL library TLS 1.0 – multiple vulnerabilities (resolution required for PCI compliance)

Resolved issues

The following issues are resolved 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.	150123

CFS

Resolved issue	Issue ID
Custom content filtering policies are not applied to users who are authenticated by Single Sign-On (SSO) with Terminal Services Agent (TSA). Instead, the default CFS policy is applied, causing web connections to be blocked for the authenticated users. Occurs when both CFS and WAN Acceleration Web Caching are enabled.	159455
Websense Enterprise is not available in the Content Filter Type drop-down list on the Security Services > Content Filter page. Occurs when the appliance has been upgraded from 5.9.0.x to 5.9.1.0.	159287
Websites load slowly when CFS is unlicensed, but enforced. UDP traffic is observed, indicating that CFS is checking website ratings. Occurs when the appliance is not licensed for CFS, while CFS is enabled on the zones being used for traffic and the Enable Allowed/Forbidden Domains checkbox is selected in the Security Services > Content Filter configuration page.	152391

DPI-SSL

Resolved issue	Issue ID
When using some types of certificates, secure (HTTPS) websites cannot be accessed using Internet Explorer. Occurs when a user certificate and its root CA are imported to SonicOS, then selected as the client’s DPI-SSL certificate, and then the firewall is rebooted.	133061

Geo IP / Botnet

Resolved issue	Issue ID
Some browsers do not accurately present the enabled/disabled state of Geo-IP Filtering. Occurs when using Internet Explorer 11 to view the Security Services > Geo-IP Filter page, which shows the "Block connections to/from countries listed in the table below" option as unchecked, even if the feature is on and actively working.	154378

Log

Resolved issue	Issue ID
Log automation does not email the logs to the designated email address when the log buffer is full or according to the schedule. The email server returns the error message, "'It was generated by qmail, an Internet message transfer agent. Your mailer tried to send an e-mail message to a server running qmail. Unfortunately, qmail spotted a problem: your mailer sent a bare LF." Occurs when the email server is hosted in the cloud, such as qmail.	154228
The full domain name of the email server is longer than the character limit for the mail server settings field, preventing automated emails. Occurs when trying to configure SonicOS to email the logs via automation and the full domain name of the email server is 40 or more characters.	150314
SSL VPN (NetExtender) user logout events do not appear in GMS reports because user authentication syslog messages are sent with the incorrect message ID. Occurs when the firewall is under GMS management and users are logging in/out with NetExtender.	146479

Networking

Resolved issue	Issue ID
Dynamic DNS settings are removed after upgrading SonicOS firmware on the appliance. Occurs when upgrading from a 5.9.0.x version to 5.9.1.0, due to a change in the dynamic DNS provider between 5.9.0.x and 5.9.1.x.	159359
An interface does not come up on an appliance which is the idle unit in a High Availability pair. The TSR shows that the interface is physically up, but the link status of it is "Down". Occurs when the Ethernet cable is disconnected from the appliance interface and the appliance is rebooted, and then the cable is reconnected to the proper interface.	154592
Auto-generated objects WAN Primary IP and All X1 Management IP are assigned an IP address of 0.0.0.0 instead of a valid public IP address. Occurs when IP Helper is enabled and the X1 interface is configured to use PPPoE with DHCP for obtaining a WAN IP address. The address objects are not updated after changing WAN mode to Static.	154587
The WAN Layer 2 Tunneling Protocol (L2TP) connection goes down and the WAN interface cannot reconnect until the appliance is restarted. Occurs when the WAN (X1) interface is working fine in L2TP mode and then L2TP server functionality is enabled on the VPN > L2TP Server page.	154203
Some dynamic and static DHCP scopes are not carried over after a firmware upgrade from 5.8.1.x to 5.9.0.x. Occurs when the DHCP scopes are configured with duplicate DNS server entries.	153442

A client computer cannot receive ARP replies for any ARP requests which cross the firewall, with the result that it cannot access the SonicOS management interface, the Internet, or even its gateway IP address. Occurs when a LAN-WAN bridge pair is configured on the firewall with X1 as the WAN Zone primary and X0 as the LAN Zone secondary, the client computer successfully connects to the SonicOS management interface from the WAN side, and then the client computer is moved from the WAN interface to the LAN interface.	146034
OSPF does not send the default route as part of its routing update; a second firewall running OSPF does not show the route in its route table after the update. Occurs when the firewall WAN interface is connected with PPPoE and "Select Originate Default Route When WAN is UP" is enabled, causing OSPF to send a routing update.	117181

SSL VPN

Resolved issue	Issue ID
SSL VPN users with one-time passwords cannot log into NetExtender. NetExtender displays the message, "Error: A temporary password has been sent to email address. Please enter it below", but does not display the field for entering the one-time password. Occurs when the NetExtender IP address pool is exhausted and NetExtender has two error conditions (one to require the one-time password and the other for the IP address pool exhaustion), but it only displays one error message.	158079
NetExtender allows VPN connections without a correct one-time password from the user. Occurs when LDAP/Active Directory and One-Time Passwords are configured in SonicOS for user authentication and a NetExtender user receives a one-time password from the system, but does not enter it correctly in the NetExtender window and is still able to log in.	155469
SSL VPN users receive a login failed error message when attempting to connect via NetExtender. Occurs when One-Time Passwords are enabled and synchronization problems occur when the email server performs some lengthy processing.	151076

System

Resolved issue	Issue ID
Imported configuration settings are lost or changed after restarting the appliance. Some user groups imported from LDAP servers disappear, routes and NAT policies are changed, and authenticated users are displayed incorrectly. Occurs when the imported user groups contain references to address objects, and those address object indexes saved to flash during import become corrupted and are not valid after reading them back. The invalid groups are then removed during the restart, causing related Access Rules and App Rules to be deleted or changed.	153607
The SonicOS web management interface and command line interface become unresponsive and a VPN connection to the appliance cannot be established, but the appliance continues to pass traffic. Occurs when a memory buffer overflow happens, such as when a large Match Object exceeds the size of the allocated memory buffer.	152125

Users

Resolved issue	Issue ID
Users are authenticated via Single Sign-On (SSO), but the Users > Status page shows the wrong groups for them. The default CFS policy is applied to all users, rather than the correct policy. If a user logs out and another user logs in from the same computer, LDAP does not return any groups. Occurs when using SSO and LDAP for user authentication in an environment such as a school where users share computers.	138291

VPN

Resolved issue	Issue ID
An SNMP walk times out over a policy based VPN with NAT applied. Occurs when two single-core firewalls, such as TZ 105, are connected with a site-to-site VPN with NAT configured on one side, and the admin tries to obtain the remote firewall information using SNMP management from a computer behind the local firewall.	150696
Traffic stops passing between the firewall and an Amazon VPC tunnel after a while. Occurs when IKE negotiation incorrectly provides the IP range instead of the subnet/mask.	150446

Vulnerability

Resolved issue	Issue ID
The SSL VPN feature in SonicOS is vulnerable to a cross site scripting attack. Occurs when performing an Acunetix scan on firmware that contains a version of jQuery older than jQuery 1.6.3.	148889

Wireless

Resolved issue	Issue ID
Wireless clients intermittently lose access to the Internet and must disable and re-enable the client wireless adaptor to regain connectivity. Occurs when the appliance is running SonicOS 5.9.1.0 and TKIP encryption is configured for the SonicPoints, rather than AES.	158318

Known issues

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

3G/4G

Known issue	Issue ID
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

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

Application Control

Known issue	Issue ID
App Rules allows configuration of policies with the same Source and Destination. Occurs when configuring a match object on Firewall > Match Objects and then on the Firewall > App Rules page configuring an App Control policy of type App Control Content that uses the match object and an Address entry.	160152
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
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

Dashboard

Known issue	Issue ID
A scheduled Appflow report sent to the FTP server is empty. Occurs when “Send Report by E-mail” is enabled together with “Send Report by FTP”.	156817

DPI-SSL

Known issue	Issue ID
The SSL proxied connection count cannot be cleared from the cache. Occurs when Client DPI-SSL is enabled and HTTPS traffic is passed through X0 and X2 which are configured in Layer 2 Bridge mode, and then X0 and X2 are changed to unassigned mode.	159332
A non-CA certificate can be configured for Client DPI-SSL. Occurs when a non-CA certificate is uploaded to the firewall and is then available in the certificate dropdown list on the DPI-SSL client configuration page.	156215
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

Networking

Known issue	Issue ID
The WAN interface cannot be accessed with HTTPS or ping after restarting the firewall. Occurs when X0 (LAN) has a redundant port configured and X0 physical status is “no link”.	156619
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
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
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
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

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
SSLVPN Enforcement on the WLAN zone redirects users to the SSL VPN portal logon page, but the logon page does not open. Occurs when browsing any HTTP website from a WLAN client machine.	161300
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
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
The LDAP connection test returns a communication error, "Error, unable to get local issuer certificate." Occurs when using a Windows LDAP server, the local certificate is imported to the firewall, the Use TLS(SSL) check box is enabled on the Users > Settings page, and then the local certificate for TLS is used when an X509 certificate is required from the server.	160393
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
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

System compatibility

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

- Dell SonicWALL WXA support
- WWAN 3G/4G support
- Browser support

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 1.3.1.

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 at https://support.software.dell.com/release-notes-product-select.

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

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

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: 6/8/2015

232-002905-00 Rev A