



# Dell SonicWALL™ SonicOS 5.9.1.6

## Release Notes

### May 2016

These release notes provide information about the Dell SonicWALL™ SonicOS 5.9.1.6 release.

- [About SonicOS 5.9.1.6](#)
- [Supported platforms](#)
- [New features](#)
- [Resolved issues](#)
- [Known issues](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading information](#)
- [Technical support resources](#)
- [About Dell](#)

## About SonicOS 5.9.1.6

SonicOS 5.9.1.6 is a maintenance release for the Dell SonicWALL network security appliances. A number of issues from previous releases are fixed in this release. See [Resolved issues](#).

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 5.9.1.x. For more information, see the previous release notes, available on MySonicWALL or on the Support Portal at: <https://support.software.dell.com/release-notes-product-select>.

# Supported platforms

The SonicOS 5.9.1.6 release is supported on the following Dell SonicWALL network security platforms:

|             |                     |          |                   |
|-------------|---------------------|----------|-------------------|
| • 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  | • SOHO   |                   |
| • NSA 3500  |                     |          |                   |

## New features

This section describes the new features in the SonicOS 5.9.1.6 release.

### SonicPoint ACe/ACi/N2 FCC new rule certification for DFS channels

Beginning in SonicOS 5.9.1.6, FCC U-NII (Unlicensed -National Information Infrastructure) New Rule (Report and Order ET Docket No. 13-49) for DFS channels is supported on SonicPoint ACe/ACi/N2 running firmware version 9.0.1.0-2. FCC U-NII New Rule compliance helps to ensure that your Dell SonicWALL wireless appliance does not interfere with other types of users in U-NII bands.

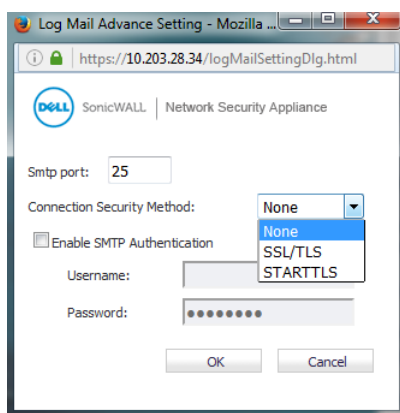
SonicPoint ACe/ACi/N2 wireless access points manufactured with FCC New Rule compliant firmware are only supported with SonicOS 5.9.1.6 and higher. Older SonicPoint ACe/ACi/N2 access points are automatically updated to the FCC New Rule compliant firmware when connected to a firewall running SonicOS 5.9.1.6 or higher.

### DPI-SSL enhancements

The DPI-SSL enhancements in SonicOS 5.9.1.6 include support for TLS 1.2 and RSA 2K/SHA-256 certificate.

## Log Automation enhancement

Log automation now supports connecting to a mail server via SSL. A new option has been added to the **Log Mail Advance Setting** dialog, **Connection Security Method**:



Select from **None**, **SSL/TLS**, or **STARTTLS**.

## Resolved issues

The following is a list of issues that are resolved in this release.

### DPI-SSL

#### Resolved issue

#### Issue ID

CFS-enabled (users and zones) DPI-SSL blocks access to Google and other sites under default CFS policy.

154670

Occurs when content filtering is enabled via users and zones with at least one custom CFS policy in addition to the default policy.

### High Availability

#### Resolved issue

#### Issue ID

Users browsing on the network encounter slow loading of browsed pages until, after approximately 120 seconds, pages do not load.

166200

Occurs when Active-Active DPI is enabled on the High Availability pair.

### IPv6

#### Resolved issue

#### Issue ID

WLAN clients cannot connect to the WAN IPv6 server, and the firewall displays the message, ICMPV6 packets too long.

167238

Occurs when W0 is configured with an IPV6 address and an IPV6 NAT policy maps the W0 private address to the X1 IPV6 public address. The X1 IPV6 MTU is set to 1500 (default). A mobile phone connected to W0 attempts to launch the Facebook app, which fails when the WLAN client sends some very large packets to the IPV6 remote server.

## Log

| Resolved issue  | Issue ID |
|---|----------|
| Attempting to email the logs or alerts on the <b>Log &gt; Log Monitor</b> page results in the error message, <code>problem connecting to your smtp server</code> .<br>Occurs when using QMail as an email server. | 157691   |

## Security Services

| Resolved issue  | Issue ID         |
|---|------------------|
| The firewall is unable to download the Geo-IP/Botnet database.<br>Occurs when the firewall encounters an unknown certificate issue while communicating with the Geo-IP/Botnet server.   | 172042           |
| App Rules allowing CFS categories for users in a certain LDAP group do not take effect, and websites are blocked for those users.<br>Occurs when a Single Sign-On user changes to inactive status, and then becomes active again upon visiting websites, which should be allowed by the App Rule. | 171848           |
| Gateway Anti-Virus does not block Microsoft Office files with macros.<br>Occurs when GAV has been configured to block Microsoft Office files containing VBA macros.   | 169124<br>149448 |
| Kaspersky is licensed on the firewall, but does not show under on the <b>Security Services &gt; Client AV Enforcement</b> page.<br>Occurs when Kaspersky is licensed on TZ 100 and TZ 100W firewalls.   | 166644           |
| Gateway Anti-Virus (GAV) does not block files containing a virus.<br>Occurs when a file containing a virus is sent as an email attachment; GAV does not block the attachment.   | 159740           |
| Websites are blocked as "Not Rated" at random times when they should be allowed according to CFS category.<br>Occurs when a spurious backslash (/) is appended to the host name by the firmware.  | 154050           |

## SSL VPN

| Resolved issue   | Issue ID |
|--|----------|
| SSL VPN connection cannot be established An SSL VPN connection cannot be established between a client device and the firewall.<br>Occurs when attempting to connect with the Mobile Connect app from iOS, Android, or Mac OS X.  | 169660   |
| NetExtender clients are frequently disconnected while transferring data, and one of several error messages displays: <ul style="list-style-type: none"><li>• <code>There was a break in the network connection</code></li><li>• <code>The connection was idle longer than configured idle timeout</code></li><li>• <code>Your user account was logged out of the SSLVPN Portal</code></li></ul> Occurs when attempting a file transfer or sending a substantial amount of traffic over the tunnel. | 169117   |
| After connecting to the network through NetExtender, clients cannot access local resources.<br>Occurs when Mac/iOS Mobile Connect clients attempt to access resources on the local network.  | 168240   |

## Upgrading

| Resolved issue   | Issue ID |
|--|----------|
| <p>TZ wireless firewalls experience WAN connectivity issues and come up in SafeMode after being power cycled.</p> <p>Occurs about 24 hours after the TZ is upgraded to SonicOS 5.9.1.5, when the Gateway Anti-Virus and IPS signature databases are automatically downloaded to the appliance.</p> | 170181   |
| <p>The firewall reboots randomly, even when no user is logged into the system.</p> <p>Occurs when the firewall is upgraded to SonicOS 5.5.1.5 HF156191.</p>  | 166533   |

## Users

| Resolved issue   | Issue ID |
|--|----------|
| <p>Incorrect/inconsistent CFS policies are applied to users.</p> <p>Occurs when different custom CFS policies are configured for different user groups.</p>  | 167483   |
| <p>Terminal Service Agent (TSA) users lose their internet connection.</p> <p>Occurs when Single Sign-On (SSO) agents report a login/logout notification to the firewall; the firewall does not check if the IP address is a TSA server, so the TSA users are authenticated twice: once as SSO/TSA and then by the SSO agent.</p> | 158910   |
| <p>Restrictive default CFS policies are enforced for users who are also members of groups that have less restrictive policies than the default CFS policies.</p> <p>Occurs when using a Citrix Terminal Server as a TSA Agent.</p>   | 142324   |

## VPN

| Resolved issue  | Issue ID |
|---|----------|
| <p>Tunnels periodically and randomly stop processing IPSec traffic.</p> <p>Occurs when using IKEv2 and dynamic VPN policy with Cisco routers.</p> | 171152   |
| <p>IKEv2 VPN tunnels (route-based VPN policy) drop randomly.</p> <p>Occurs when both IPv4 and IPv6 are received with Microsoft Azure.</p>         | 157568   |

## Vulnerability

| Resolved issue  | Issue ID |
|---|----------|
| <p>Firewalls may be vulnerable to a FireStorm cyberattack.</p> <p>Occurs when a full TCP handshake is permitted regardless of the packet destination.</p>   | 168014   |
| <p>Vulnerability Assessment and Penetration Testing fails a test for Clickjacking.</p> <p>Occurs when users click on links on a site, but the links have been "clickjacked." Clickjacking, also known as a UI redress attack, is a method in which an attacker uses multiple transparent or opaque layers to trick a user into clicking a button or link on a page other than the one they believe they are clicking. Thus, the attacker is "hijacking" clicks meant for one page and routing the user to an illegitimate page.</p> | 160432   |
| <p>When running a vulnerability scan, the scan fails with a <code>TCP Sequence Number Approximation Based Denial of Service message with code CVE-2004-0230</code>.</p> <p>Occurs when SonicOS receives a TCP SYN bit set in the synchronized state.</p>  | 152336   |

# 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.<br>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   |

## AppFlow

| Known issue   | Issue ID |
|---|----------|
| The <b>Create Rule</b> option on the <b>Users</b> tab in <b>Dashboard &gt; AppFlow Monitor</b> does not work correctly, and log messages are displayed on the console.<br>Occurs when attempting to create a rule for a RADIUS user to block LAN to WAN access, when the user already belongs to a group that has LAN to WAN access.              | 167772   |
| SSL VPN users are not displayed in <b>Dashboard &gt; AppFlow Monitor</b> on the <b>Users</b> tab, only “unknown” users are shown.<br>Occurs when several (10) SSL VPN users are connected to the firewall and AppFlow Reporting is enabled.   | 167149   |
| IPv6 applications are not displayed in the <b>AppFlow Monitor</b> page.<br>Occurs when some IPv6 streams have been triggered by visiting certain websites.  | 166912   |
| The <b>Dashboard &gt; AppFlow Reports</b> page does not display any entries on the <b>Applications</b> tab.<br>Occurs when <b>Flow Reporting</b> , <b>Real-Time Data Collection</b> , and <b>AppFlow To Local Collector</b> are enabled, and some HTTP/FTP/ICMP connections are made on the LAN side. <b>AppFlow Monitor</b> shows some sessions. | 164502   |

## Application Control

| Known issue   | Issue ID |
|---|----------|
| <p>The App Rule Match Object cannot match a filename.</p> <p>Occurs during an FTP download or upload and the <b>Match Type of the Firewall &gt; Match Object</b> is set to <b>Prefix Match</b>, the <b>Input Representation</b> is set to <b>Hexadecimal Representation</b>, and the <b>Enable Negative Matching</b> option is selected.</p> <p><b>Workaround:</b> Do not enable the Negative Matching option with the Prefix Match option.</p>             | 135634   |
| <p>App Control policies do not block IPv6 traffic unless Intrusion Prevention Service (IPS) is enabled.</p> <p>Occurs when IPS is disabled and an App Control policy is created from <b>Firewall &gt; App Control Advanced</b> to block FTP traffic. A computer on the LAN side can still use an IPv6 IP address to connect to an FTP server.</p> <p><b>Workaround:</b> Enable IPS. With IPS enabled, the App Control policy blocks the FTP connection.</p> | 128410   |

## Command Line Interface

| Known issue  | Issue ID |
|--|----------|
| <p>The CLI incorrectly indicates that Gateway Anti-Virus is not licensed.</p> <p>Occurs when using the <code>show status</code> CLI command while GAV is licensed on the appliance.</p>  | 160800   |
| <p>Access Rules are not removed on the Backup device of an HA pair and further configuration is not synchronized with the Backup device.</p> <p>Occurs when the <code>access-rule restore-defaults</code> CLI command is issued.</p> | 141949   |

## DPI-SSL

| Known issue  | Issue ID |
|--|----------|
| <p>The SSL proxied connection count cannot be cleared from the cache.</p> <p>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.</p>   | 159332   |
| <p>The certificate from a secure website, such as <code>https://mail.google.com</code>, is not changed to a Dell SonicWALL DPI-SSL certificate as it should be, and traffic cannot be inspected.</p> <p>Occurs when the <b>Enable SSL Client Inspection</b> option is set on the <b>DPI-SSL &gt; Client SSL</b> 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.</p> | 123097   |

## IPv6

| Known issue   | Issue ID |
|---|----------|
| <p>A 6rd tunnel (IPv6 rapid deployment tunnel) is unexpectedly reported as UP although there is no available 6rd prefix.</p> <p>Occurs when the tunnel was previously UP and using DHCP mode, and then the DHCP server is disabled and the firewall is rebooted.</p>  | 157034   |
| <p>IPv6 traffic that is sent over a 6rd interface is not forwarded.</p> <p>Occurs after rebooting the firewall.</p> <p><b>Workaround:</b> Go to the <b>Network &gt; Interfaces</b> page, open the <b>Edit Interface</b> dialog for the 6rd interface, and click <b>OK</b> without making any changes. Traffic should be forwarded after that.</p> | 143079   |

| Known issue  | Issue ID |
|--|----------|
| IPv6 packets exceeding the Maximum Transmission Unit (MTU) are dropped instead of being fragmented.<br>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.<br>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 |
|---|----------|
| 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.<br>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.<br><b>Workaround:</b> Restart the firewall to make X1 accessible again. | 160164   |
| The WAN interface cannot be accessed with HTTPS or ping after restarting the firewall.<br>Occurs when X0 (LAN) has a redundant port configured and X0 physical status is “no link”.   | 156619   |
| The default route gateway is wrong after changing the WAN mode.<br>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.                       | 154144   |
| The paired interface does not go down when the other interface in the Wire Mode pair is brought down.<br>Occurs when the <b>Enable Link State Propagation</b> 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.<br>Occurs when configuring OSPFv3 from the <b>Network &gt; Routing</b> page. IPv6 default route origination via OSPFv3 is currently not supported.   | 150771   |
| Disabling one DHCPv6 client also disables another DHCPv6 client.<br>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.<br>Occurs when the destination link-local IPv6 address is the same as the Wire mode interface address.  | 144385   |
| The default gateway cannot be configured.<br>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.<br>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.<br>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.<br>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 |
|--|----------|
| <p>Excluding users for an individual Intrusion Prevention signature does not work as expected.</p> <p>Occurs when Security Services &gt; Intrusion Prevention is enabled for all signatures, and IPS is also enabled for the WAN and LAN zones, and then the administrator configures a user in Excluded Users/Groups for a particular signature ID. When traffic containing that signature is sent by that user from the WAN side to a computer on the LAN, the log shows that the traffic was blocked by IPS and the user's name appears in the log.</p> | 160458   |
| <p>SonicOS drops the Client CFS Ping reply packets, and Client CFS Enforcement does not work on the SSL VPN zone.</p> <p>Occurs when the source IP address of the Client CFS Ping packet is the WAN interface IP address.</p>  | 135585   |
| <p>The Gateway AV Exclusion List does not prevent some IP addresses from being blocked.</p> <p>Occurs when an FQDN Address Object is included in the Gateway AV Exclusion List.</p>  | 121984   |

## SSL VPN

| Known issue   | Issue ID |
|---|----------|
| <p>SSLVPN Enforcement on the WLAN zone redirects users to the SSL VPN portal logon page, but the logon page does not open.</p> <p>Occurs when browsing any HTTP website from a WLAN client machine.</p> | 161300   |

## System

| Known issue   | Issue ID |
|---|----------|
| <p>The configuration mode on the LCD panel cannot be accessed and displays an Invalid Code error message.</p> <p>Occurs when the administrator selects the Configuration option on the LCD panel and enters the new PIN code that was just changed on the <b>System &gt; Administration</b> page.</p>   | 130379   |
| <p>Dell SonicWALL GMS does not synchronize with SonicOS after making password changes in One Touch Configuration and then rebooting the appliance.</p> <p>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.</p> | 124998   |
| <p>The management computer cannot manage the firewall because SonicOS cannot forward Ethernet packets larger than 1496 KB.</p> <p>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.</p>   | 121657   |

## User Interface

| Known issue  | Issue ID |
|--|----------|
| <p>The <b>Latest Alerts</b> section of the <b>System &gt; Status</b> page does not display any alerts.</p> <p>Occurs when interfaces are enabled or disabled, or when other events occur that are known to cause alerts.</p> | 160868   |
| <p>The hyperlink in "Click <a href="#">here</a> for UTM management" does not work.</p> <p>Occurs when logged into the IPv6 address of the SSL VPN Virtual Office portal.</p>   | 157523   |

## VoIP

| Known issue   | Issue ID |
|---|----------|
| <p>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.</p> <p>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.</p> | 128225   |

## VPN

| Known issue   | Issue ID |
|---|----------|
| <p>A client behind the central firewall can ping a LAN device behind the remote firewall even though the device is in the “excluded LAN devices” table.</p> <p>Occurs when the remote firewall is configured to use DHCP over VPN and the LAN device is first configured as a “static device on LAN” on the remote firewall and then added to the “excluded LAN devices” table.</p>   | 166617   |
| <p>VPN negotiation fails and the log for the Initiator does not have an entry showing “IKEv2 negotiation complete”.</p> <p>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.</p>   | 148167   |
| <p>Traffic goes to the wrong VPN tunnel.</p> <p>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.</p> <p>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.</p> <p>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.</p> | 135205   |
| <p>An active IPv6 VPN tunnel is not displayed in the table on the <b>VPN &gt; Settings</b> page of the head-end firewall.</p> <p>Occurs when two IPv6 VPN tunnels are created on both the head-end appliance and a remote appliance. The head-end <b>VPN &gt; Settings</b> page shows “2 Currently Active IPv6 Tunnels”, but it only displays one tunnel in the Currently Active VPN Tunnels table.</p>   | 128633   |
| <p>An OSPF connection cannot be established between an NSA 240 and an NSA 7500.</p> <p>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.</p>   | 128419   |

# System compatibility

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

## Wireless 3G/4G broadband devices

SonicOS 5.9.1.6 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/supported-wireless-broadband-cards-devices/>.

- i** **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.

## GMS support

Dell SonicWALL Global Management System (GMS) 7.2 Service Pack 5 (or higher 7.2) or GMS 8.1 (or higher) are required for GMS management of Dell SonicWALL SOHO appliances running SonicOS 5.9.1.6.

## 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 5.9.1.6. 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 (do not use compatibility mode)
- Safari 5.0 and higher running on non-Windows machines

- i** **NOTE:** On Windows machines, Safari is not supported for SonicOS management.

- i** **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.

# 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 at <https://mysonicwall.com/> or on the Support portal at <https://support.software.dell.com/>.

**IMPORTANT:** If VPN tunnel interfaces are configured on your appliance running SonicOS 5.8, be sure to read the “Upgrading caveats for VPN tunnel interfaces” section in the *SonicOS 5.9 Upgrade Guide* before upgrading your appliance to SonicOS 5.9.

# 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 Support Portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to <http://support.software.dell.com>.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles at:  
<https://support.software.dell.com/kb-product-select>
- Obtain product notifications
- View how-to videos at:  
<https://support.software.dell.com/videos-product-select>
- Engage in community discussions
- Chat with a support engineer

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 <http://www.software.dell.com>.


# Contacting Dell


For sales or other inquiries, visit <http://software.dell.com/company/contact-us.aspx> or call 1-949-754-8000.


Copyright © 2016 Dell Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. Dell™, the Dell logo, and SonicWALL are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

---

Last updated: 5/2/2016

232-003225-00 Rev A