

SonicWall™ SonicOS 6.2.9.0

Release Notes

July 2017

These release notes provide information about the SonicWall™ SonicOS 6.2.9.0 release.

Topics:

- [About SonicOS 6.2.9.0](#)
- [Supported Platforms](#)
- [New Features](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [System Compatibility](#)
- [Product Licensing](#)
- [Upgrading Information](#)
- [SonicWall Support](#)

About SonicOS 6.2.9.0

SonicWall SonicOS 6.2.9.0 provides new features and fixes various known issues found in previous releases. For more information, see the [New Features](#) and [Resolved Issues](#) sections.

Supported Platforms

SonicOS 6.2.9.0 is supported on the following SonicWall appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ300 / TZ300 Wireless
- SOHO Wireless

New Features

This section describes the new features introduced in SonicOS 6.2.9.

NOTE: SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.2.9 requires GMS 8.3.1 (8.3 Service Pack 1) for management of firewalls using the new features in SonicOS 6.2.9.

Topics:

- [Increased SPI/DPI Connections Capacity](#)
- [DPI vs DPI-SSL Dynamic Connection Sizing](#)
- [Active/Active Clustering on NSA 3600 & 4600](#)
- [Enhanced HTTP/HTTPS Redirection](#)
- [Capture ATP User Experience Enhancements](#)

Increased SPI/DPI Connections Capacity

SonicOS 6.2.9 increases the maximum number of Stateful Packet Inspection (SPI) and Deep Packet Inspection (DPI) connections supported on NSA 2600-6600 and SuperMassive 9200-9600 platforms. You can enable SPI or DPI connections on the **Firewall Settings > Advanced** page in SonicOS.

The [SPI Previous vs New Maximum Connections](#) table shows the previous maximums and new target maximums for the number of connections supported on each platform with SPI enabled.

SPI Previous vs New Maximum Connections

Platform	Previous Maximum Connections	New Maximum Connections
NSA 2600	225,000	500,000
NSA 3600	325,000	750,000
NSA 4600	400,000	1,000,000
NSA 5600	750,000	1,500,000
NSA 6600	750,000	1,500,000
SM 9200	1,250,000	5,000,000
SM 9400	1,250,000	7,500,000
SM 9600	1,500,000	10,000,000

For appliances with DPI enabled, the [DPI Previous vs New Maximum Connections](#) table shows the previous maximums and new target maximums for the number of connections supported on each platform.

DPI Previous vs New Maximum Connections

Platform	Previous Maximum Connections	New Maximum Connections
NSA 2600	125,000	250,000
NSA 3600	175,000	375,000
NSA 4600	200,000	500,000
NSA 5600	500,000	1,000,000
NSA 6600	500,000	1,000,000
SM 9200	1,000,000	1,500,000

DPI Previous vs New Maximum Connections

Platform	Previous Maximum Connections	New Maximum Connections
SM 9400	1,000,000	1,500,000
SM 9600	1,250,000	2,000,000

To select the connection mode (SPI or DPI) for the firewall:

- 1 Navigate to the **Firewall Settings > Advanced** page.
- 2 In the **Connections** section, select one of the following radio buttons:
 - **Maximum SPI Connections (DPI services disabled)** — Enables Stateful Packet Inspection. This option allows the most simultaneous connections, but does not provide as much security as Deep Packet Inspection.
 - **Maximum DPI Connections (DPI services enabled)** — Enables Deep Packet Inspection. This is the default and recommended setting for most SonicWall network security appliance deployments.
 - **DPI Connections (DPI services enabled with additional performance optimizations)** — Enables Deep Packet Inspection with increased firewall DPI inspection throughput and fewer overall DPI connections. This option is intended for performance critical deployments.
- 3 Click **Accept** at the top of the page.
- 4 Restart the firewall. Any change to the Connection settings requires a restart for the changes to take effect.

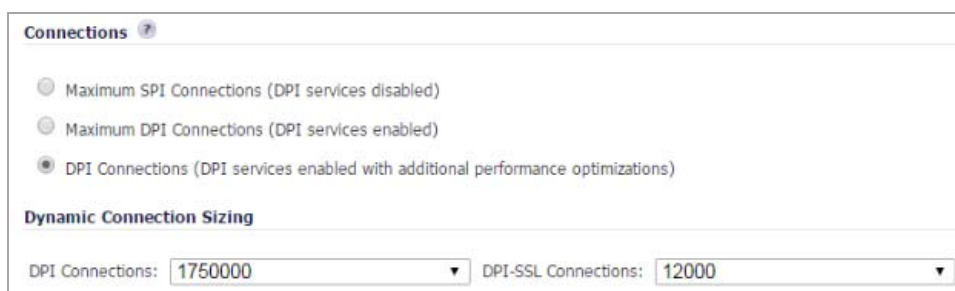
DPI vs DPI-SSL Dynamic Connection Sizing

For the products that support more than 250,000 DPI connections (NSA 2600 and higher), there is an option to adjust the number of desired DPI vs DPI-SSL connections. For every 125,000 DPI connections reduced, the number of available DPI-SSL connections increases by 750. For example:

- A reduction of 250,000 DPI connections results in an increase of 1,500 additional DPI-SSL connections.
- A reduction of 500,000 DPI connections results in an increase of 3,000 additional DPI-SSL connections.

To configure a reduction in DPI connections:

- 1 Navigate to the **Firewall Settings > Advanced** page.
- 2 On NSA and SuperMassive platforms, the **Dynamic Connection Sizing** section is displayed below **Connections**.



The screenshot shows the 'Connections' section of the Firewall Settings > Advanced page. It features three radio button options: 'Maximum SPI Connections (DPI services disabled)', 'Maximum DPI Connections (DPI services enabled)', and 'DPI Connections (DPI services enabled with additional performance optimizations)'. Below this is the 'Dynamic Connection Sizing' section, which contains two dropdown menus: 'DPI Connections' set to 1750000 and 'DPI-SSL Connections' set to 12000.

- NOTE:** This setting is only available when one of the following options is selected under **Connections**:
- **Maximum DPI Connections (DPI services enabled)**
 - **DPI Connections (DPI services enabled with additional performance optimizations)**

- 3 Using the **DPI Connections** drop-down list, adjust the desired number of DPI connections.
For every 125,000 DPI connections reduced, the maximum number of DPI-SSL connections increases by 750.
- 4 Alternatively, adjust the desired number of DPI-SSL connections with the **DPI-SSL Connections** drop-down list.
- 5 Click **Accept** at the top of the page.

Active/Active Clustering on NSA 3600 & 4600

SonicOS 6.2.9 extends support for Active/Active Clustering to the NSA 3600 and NSA 4600 platforms.

In this mode, multiple firewalls are grouped together as cluster nodes, with multiple Active units processing traffic (as multiple gateways), doing DPI and sharing the network load.

Each cluster node consists of two units acting as a Stateful HA pair. Active/Active Clustering provides Stateful Failover support in addition to load-sharing. Optionally, each cluster node can also consist of a single unit, in which case Stateful Failover and Active/Active DPI are not available.

 **NOTE:** As with NSA 5600 and 6600, Active/Active Clustering is supported on NSA 3600 and NSA 4600 platforms only with the purchase of a SonicOS Expanded License.

Enhanced HTTP/HTTPS Redirection

This feature solves an issue where the firewall Control Plane (CP) can become overloaded with HTTP/HTTPS redirection requests to the point where it slows SonicOS management access.

Normally, when the firewall configuration requires user authentication, HTTP/HTTPS traffic from an unauthenticated source is redirected to the SonicOS login screen and then the user enters their credentials. The problem occurs when HTTP and HTTPS traffic arrives from sources from which users do not log in, and one or more such sources repeatedly try to open new connections that keep triggering this redirection. These could be non-user devices that are validly trying to get access, or could be malicious code attempting a Denial of Service (DOS) attack. The effect that it has on the firewall is to cause high CPU load in the CP; both in the data plane task initiating the redirections, and in the web server thread tasks that are serving up the target redirect pages.

The **Add rule to enable redirect from HTTP to HTTPS** checkbox should be enabled for best results. This checkbox is found in the **Edit Interface** dialog when editing a physical interface from the **Network > Interfaces** page, depending on the **Mode/IP Assignment** setting. You can also set this option in the **Add Interface** dialog when adding a Virtual Interface or a WLAN Tunnel Interface.

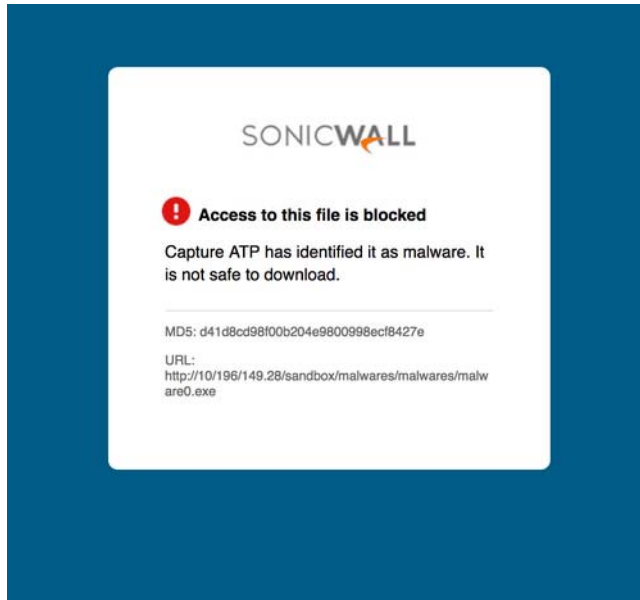
Enabling this checkbox causes SonicOS to add an access rule that allows HTTP to the interface so that it can be redirected to HTTPS, and a side effect of this is that it also allows SonicOS to be able to redirect HTTPS to HTTP in certain cases where that has no security issues. One such case is the first step of redirecting traffic that needs to be authenticated, at which point there is no sensitive data that needs to be hidden. Then, the HTTP processing can occur on the data plane (DP) rather than on the CP.

Capture ATP User Experience Enhancements

The SonicWall Capture ATP **Block** and **Pending** pages are updated with a new look and feel.

The Block page appears when Capture ATP has identified a file as unsafe due to malware, and blocks the download.

Block Page



NOTE: The Block page is applicable only when the **Block file download until a verdict is returned** option is selected in the **Custom Blocking Behavior** section of the **Capture ATP > Settings** page.

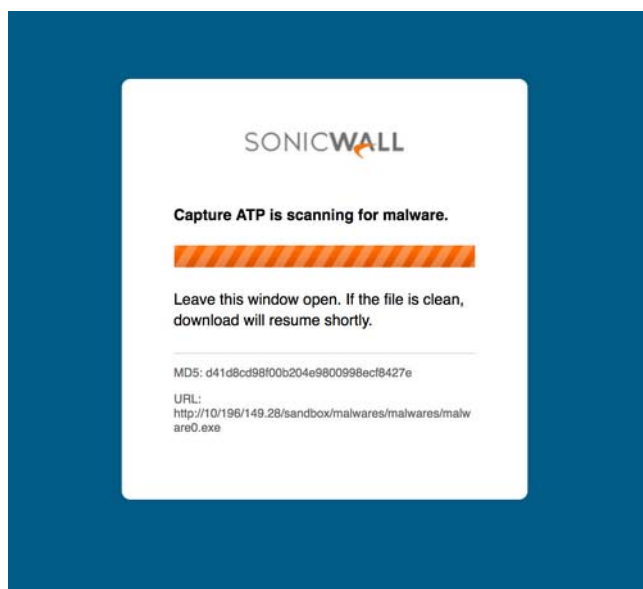
Custom Blocking Behavior

Files that are not identified as malicious by other security services on the firewall will be sent to Capture ATP cloud service for analysis.

- Allow file download while awaiting a verdict
Will allow file download without delay and the Capture service will analyze the file in parallel for malicious behavior. You will be alerted via email and in firewall logs if the Capture service analysis determines that the file is malicious.
- Block file download until a verdict is returned
Will delay file download until a verdict is reached by the Capture service. This affects legitimate files as well as potentially malicious files and may require users to retry the download.
Note: Only applies to HTTP/S file downloads

The Pending page appears when Capture ATP begins scanning a file for malware. The progress bar fills in as the file is scanned, refreshing every 30 seconds.

Pending Page



Resolved Issues

This section provides a list of resolved issues in this release.

Bandwidth Management

Resolved issue	Issue ID
Bandwidth Management is not working with Content Filtering for HTTPS sites. Occurs when Client DPI-SSL is enabled and the content filter settings are configured on the DPI-SSL > Client SSL page under CFS Category-based Exclusion/Inclusion .	189258

CFS

Resolved issue	Issue ID
Domains included in the Forbidden URI list in CFS 3.0, but not being blocked, are added to the Forbidden URI List in CFS 4.0 and are then blocked. Occurs when upgrading from CFS 3.0 to CFS 4.0 after configuring a Forbidden URI list and disabling the Block Access to URL option.	185082
Cannot use FQDN Address Objects or MAC Address Object for the Source address of a CFS policy. Occurs because MAC and FQDN Address objects were not previously supported when creating CFS policies.	184034

DPI-SSL

Resolved issue	Issue ID
Server DPI-SSL Address Object Certificate pair disappears and re-appears randomly in the SonicOS web management interface. Occurs when DPI-SSL does not sync correctly after the Address Object is modified or deleted	186564
HTTPS downloads and HTTPS websites are slow and can fail, while other throughput is also slow. Occurs when Client DPI-SSL is enabled and applied to a host and then the host tries to access HTTPS sites and download files over HTTPS.	172063

Gateway Anti-Virus

Resolved issue	Issue ID
Many GAV Alerts are generated with the message "Gateway Anti-Virus Alert: SMB out of order read/write". Occurs when CIFS/NetBIOS scanning is enabled on GAV, and then a shared folder on PC2 is accessed from PC1 using SMB2.	175366

High Availability

Resolved issue	Issue ID
Failover occurs if a Link AggregationGroup (LAG) parent interface is down. Occurs when a Stateful HA pair has two ports in the LAG, and the Active/Standby Failover only when ALL aggregate links are down option is enabled. HA physical link monitoring is enabled on a VLAN whose physical interface is the parent link aggregated port. The switch is used to disable a non-parent LAG interface of the active firewall, then that interface is turned back on and the parent LAG interface is disabled.	188765
High Availability between units fails when the admin password is longer than 31 characters. Occurs when the password contains 32 or more characters.	182901

Log

Resolved issue	Issue ID
Columns are misaligned with column headers on the Log Monitor page. Occurs when a Capture log message affects the alignment.	189524

Networking

Resolved issue	Issue ID
IPv6 FQDN Network Monitor policies are lost after restarting the firewall. Occurs when the IPv6 FQDN Network Monitor policies have a comment included in their configuration.	185079
When adding an access rule in Firewall > Access Rules, using the option to create a new address object prevents the rule from being saved. Occurs when using the Internet Explorer 11 browser to manage the appliance.	185057
Active or passive FTP does not work with NAT64 when specifying the outbound interface. Occurs when the specified outbound interface is affected by a NAT64 policy.	184889
An access rule with a schedule will change its schedule after rebooting. Occurs when two schedule objects are available and the access rule is configured to use one of them. After the reboot, the rule table shows the access rule using the other schedule.	184803

Networking

Resolved issue	Issue ID
<p>The Enable DNS Proxy option becomes disabled or disappears after the WLAN tunnel interface is saved and then edited again.</p> <p>Occurs when the global Enable DNS Proxy option is enabled and then a WLAN tunnel interface is added with the same option selected in its configuration. After saving the tunnel interface configuration, the Enable DNS Proxy option is shown as disabled or disappeared when checking the tunnel interface settings.</p>	184385
<p>An IPv6 host resolved in an IPv6 MAC Address Object does not disappear after modifying that MAC address to a new value in a static NDP entry.</p> <p>Occurs when a MAC AO resolves an IPv6 address from a static NDP table, then one NDP entry's MAC address is changed to a new value, and find that the previously resolved IPv6 address is still displayed in the MAC AO.</p>	184318
<p>An active TCP Connection is dropped with the error, "Access Rule Policy Not Found".</p> <p>Occurs when TCP is allowed by an access rule whose destination is an FQDN Address Object whose TTL is short and expires while traffic is flowing.</p>	183862

SSL VPN

Resolved issue	Issue ID
<p>An RDP5 Java bookmark connection incorrectly stays connected and the entire subnet is accessible via RDP client.</p> <p>Occurs when the original bookmark user has logged out from the portal, but the user did not disconnect the RDP session.</p>	153489

System

Resolved issue	Issue ID
<p>The firewall reboots at random times.</p> <p>Occurs when memory exhaustion in the SSL VPN functional area occurs, although the overall memory situation is still healthy.</p>	188194
<p>SonicOS cannot disable or enable a NAT64 policy.</p> <p>Occurs when a few NAT policies already exist.</p>	183304
<p>The firewall reboots due to a DP core timeout.</p> <p>Occurs when there is very heavy use of the SonicOS web UI for user level authentication.</p>	168037

User Interface

Resolved issue	Issue ID
<p>Duplicate route policies are created when editing a route policy on an NSA 2600.</p> <p>Occurs when editing a route policy and clicking the OK button repeatedly in the Edit Route Policy dialog when the firewall does not respond immediately.</p>	188525
<p>A non-printing space character representation, "&nbsp;" is displayed.</p> <p>Occurs when viewing the Firewall Settings > BWM page, in the Priority column for all priorities.</p>	188417
<p>Firewall Access Rules appear modified or blank. For example, custom rules can change from "LAN > WAN" to "0 > WAN" and the administrator cannot enable, disable, or change the modified rules.</p> <p>Occurs when the Access Rule comments include a comma or vertical bar ' ' symbol and then the firmware is upgraded to 6.2.7.1. It is possible that other characters may have a similar effect.</p>	185528

Wizards

Resolved issue	Issue ID
The Setup Guide wizard contains the incorrect statement, “Since HA is enabled, only Static IP addressing is allowed”. In SonicOS 6.2.9, Dynamic WAN interfaces are supported in High Availability mode. Occurs in the WAN Mode screen of the wizard.	184891

Known Issues

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

3G/4G

Known issue	Issue ID
Web browsing and 1MB FTP downloads are slower on SonicOS 6.2.9.0 than on 6.2.6.0. Occurs when connected to WWAN with a Sprint 3G card.	183961

Capture ATP

Known issue	Issue ID
The UFTP retransmit buffer is not 10MB by default, but it should be for best performance. Occurs when Capture ATP is transmitting files to the servers for scanning and analysis.	190106

High Availability

Known issue	Issue ID
In a High Availability deployment with one unit down, the active appliance becomes unresponsive. Occurs when heavy, mixed traffic including SIP (H.323) traffic is passing through the active appliance, while the other unit in the HA pair is powered down.	190464

IPv6

Known issue	Issue ID
SonicOS sends IPv4 DNS requests when communicating with SonicWall backend servers such as MySonicWall or the License Manager. Occurs when the X1 (WAN) interface and the DNS server are only configured with IPv6 addresses.	183975

Networking

Known issue	Issue ID
Routes are not learned between two firewalls connected with VPN Tunnel Interfaces. Occurs when using advanced routing with RIPv1.	189538
A newly added IPv6 rule is incorrectly placed before IPv4 rules. Occurs when the IPv6 rule is from LAN to VPN or VPN to LAN.	189445
When using NAT64, HTTPS traffic fails in some cases. Occurs when SSL Client Inspection is enabled.	184830

Networking

Known issue	Issue ID
<p>A specific sub-domain host IP address cannot be added into a FQDN Address Object.</p> <p>Occurs when a FQDN AO such as *.e.com is added, then the admin queries 1.e.com, 2.e.com, and 3.e.com on a computer connected to the firewall LAN zone and the IP addresses for those sub-domains are returned by the server. But, the FQDN AO still only contains the host IP address for e.com.</p>	184156
<p>A sub-VLAN interface configured in PPPoE/PPTP/L2TP mode and then changed cannot connect again during the enabled schedule.</p> <p>Occurs when the interface is changed to static mode while connected, and then changed back to iPPPoE/PPTP/L2TP mode.</p>	183607

SonicPoint

Known issue	Issue ID
<p>RADIUS Accounting can be configured with a SonicPoint NDR access point, but then no accounting messages reach the accounting server.</p> <p>Occurs when SonicOS allows configuration of the Radius Accounting settings with older SonicPoint platforms that are not officially supported.</p>	181522

SSL VPN

Known issue	Issue ID
<p>Closing a VNC bookmark logs the user out of the SSL VPN portal.</p> <p>Occurs when the user closes the bookmark.</p>	189314

Switching / X-Series

Known issue	Issue ID
<p>In an HA pair, importing settings after an X-series switch is deleted clears the VLAN configuration in the switch.</p>	183564

VPN

Known issue	Issue ID
<p>A VPN policy which is already used in an existing Tunnel Interface is incorrectly shown in the drop-down list.</p> <p>Occurs when a new Tunnel Interface is being added and the policy choices are viewed in the VPN Policy drop-down list.</p>	189220
<p>Only one of two protected subnets behind an Auto Provisioning (AP) client can establish a tunnel to the AP server.</p> <p>Occurs when the AP server policy has the Require Authentication of VPN AP Clients via XAUTH option enabled. If the Allow Unauthenticated VPN AP Client Access option is enabled instead, both subnets can establish a tunnel.</p>	185074
<p>The VPN Tunnel cannot be negotiated in some cases.</p> <p>Occurs when the Auto-Provisioned Server uses a certificate with a wildcard character in the DN and the DN also includes ID strings using "DC=".</p>	181322

Wireless

Known issue	Issue ID
Multiple wireless clients cannot access the internet at the same time using Lightweight Hotspot Messaging. Occurs when one of following sequences takes place: <ul style="list-style-type: none">Wireless Client1 tries to access the internet, is redirected to the login page and logs in successfully. Wireless Client2 tries to access the internet, is redirected to the login page, but gets a “Session creation failed” error and cannot log in.Wireless Client1 tries to access the internet, the page is redirected to the login page, but Client1 does not log in right away. Then, Wireless Client2 tries to access the internet, the page is redirected to the login page and Client2 logs in. The result is that Client1 is authenticated and can access the internet successfully, while Client2 is asked to log in every time while trying to access the internet.	190413

System Compatibility

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

Wireless 3G/4G Broadband Devices

SonicOS 6.2.9 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/>.

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.2.9 requires GMS 8.3.1 for management of firewalls using the new features in SonicOS 6.2.9. SonicWall GMS 8.3 supports management of all other features in SonicOS 6.2.9 and earlier releases.

WAN Acceleration / WXA Support

The SonicWall WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with SonicWall security appliances running SonicOS 6.2.9. 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. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 18.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 16.0 and higher
- Internet Explorer 9.0 and higher
- Safari 5.0 and higher running on non-Windows machines

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

NOTE: Mobile device browsers are not recommended for SonicWall appliance system administration.

Product Licensing

SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at <https://mysonicwall.com>.

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the *SonicOS 6.2 Upgrade Guide* available on the Support portal at <https://www.sonicwall.com/en-us/support/technical-documentation>.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products 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. To access the Support Portal, go to <https://www.sonicwall.com/en-us/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/en-us/support/contact-support>.

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/en-us/legal/license-agreements>. Select the language based on your geographic location to see the EUPA that applies to your region.


Copyright © 2017 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' 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 SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME 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 SONICWALL AND/OR ITS AFFILIATES 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 SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal/>.

Legend

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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

Last updated: 7/28/17

232-003986-00 Rev A