



Dell SonicWALL™ SonicOS 6.1.1.12

Release Notes

November 2015

These release notes provide information about the Dell SonicWALL SonicOS 6.1.1.12 release.

Topics:

- [About SonicOS 6.1.1.12](#)
- [Supported platforms](#)
- [Resolved issues](#)
- [Known issues](#)
- [System compatibility](#)
- [Product licensing](#)
- [Upgrading information](#)
- [Technical support resources](#)
- [About Dell](#)

About SonicOS 6.1.1.12

SonicOS 6.1.1.12 is a maintenance release that fixes certain known issues including the RSA-CRT vulnerability. See [Resolved issues](#).

This release provides all the features and contains all the resolved issues that were included in previous releases of SonicOS 6.1.1.x. For more information, see the previous release notes on MySonicWALL at <https://mysonicwall.com/> or on the Support portal at <https://support.software.dell.com/>.

i **IMPORTANT:** SonicOS 6.1.1.10, 6.1.1.11 and 6.1.1.12 include a *design change* for the treatment of traffic over VPN tunnel interfaces. By default, NAT policies are now applied to this traffic. In SonicOS 6.1.1.9 and earlier 6.1.1.x releases, traffic over VPN tunnel interfaces was exempt from NAT policies. Upgrading from one of these earlier releases to 6.1.1.12 may require configuration changes if you are using VPN tunnel interfaces.

Supported platforms

The SonicOS 6.1.1.12 release is supported on the following Dell SonicWALL network security appliances:

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600

Resolved issues

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

System

Resolved issue	Issue ID
<p>A specialized RSA-CRT attack can cause private key leakage in relatively rare cases. This security vulnerability has not been publically disclosed and it is very difficult to perform this attack. To be cautious, Dell SonicWALL recommends that customers upgrade firmware.</p> <p>Occurs when the SonicOS management interface or a port on the firewall is accessed using SSL, and the following conditions are met:</p> <ul style="list-style-type: none">• A highly sophisticated tool is used to harvest this vulnerability; this tool is not available to the general public• The Enable Hardware RSA option is enabled in the internal SonicOS settings (by default this option is disabled, in which case the firewall is not vulnerable)	166825
<p>SonicOS web-based management becomes inaccessible via the MGMT port.</p> <p>Occurs when CPU utilization is 100% while waiting for processing that cannot complete due to an error condition.</p>	165687
<p>The firewall restarts repeatedly with DP core 30 exceptions shown in the TSR.</p> <p>Occurs when Client DPI-SSL is enabled and errors occur when signatures are downloaded.</p>	157272

Known issues

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

AppFlow

Known issue	Issue ID
<p>A JavaScript error is shown in a popup with the heading, "Errors on this webpage might cause it to work incorrectly", and no URLs can be displayed on the URLs tab of the AppFlow > AppFlow Monitor page in SonicOS.</p> <p>Occurs when the Enable AppFlow To Local Collector option is fully enabled for AppFlow > Flow Reporting, users have accessed web pages from the LAN, and Internet Explorer 9 is used to view the AppFlow > AppFlow Monitor page in SonicOS.</p>	164241

Application Control

Known issue	Issue ID
<p>App Control Advanced does not block the Psiphon client in SSH+ mode.</p> <p>Occurs when Client DPI-SSL is enabled with Intrusion Prevention and App Control is enabled on relevant zones and configured to block Psiphon with Category set to Proxy-Access and several Signatures enabled, including SID 5, 7486, 10330, 10517, and 10097.</p>	162055
<p>The Ultrasurf browser plugin is not blocked by an App Rule or App Control Advanced.</p> <p>Occurs when using the Chrome browser plugin for Ultrasurf.</p>	161651
<p>App Control does not block access to Google Play app store from a smartphone app, but <i>play.google.com</i> is blocked from a browser on a personal computer.</p> <p>Occurs when DPI-SSL is not enabled and an App Rule is configured on the firewall to block the Google Play application and signatures, then an Android smartphone connects to the firewall via a wireless access point and can download or update apps from the Google Play store.</p>	157692
<p>The Firewall Settings > BWM link in an App Rule does not display the correct page.</p> <p>Occurs when configuring a new policy in the App Rules page and clicking the Firewall Settings > BWM link.</p>	153370

DPI-SSL

Known issue	Issue ID
<p>The Google Drive desktop application cannot connect or synchronize with the Google Drive servers.</p> <p>Occurs when Client DPI-SSL is enabled. The Google Drive application uses a pinned certificate for speed and accessibility, but DPI-SSL re-writes the certificate and signs it with the firewall certificate authority (CA), or uses a different certificate if specified. The Google Drive application rejects the rewritten certificate with an "Unknown CA" error.</p> <p>Workaround: Exclude the following domains from DPI-SSL:</p> <ul style="list-style-type: none">• .google.com• .googleapis.com• .gstatic.com <p>Because Google uses the same certificate for all its applications, this excludes all Google applications from DPI-SSL inspection.</p>	162719

Log

Known issue	Issue ID
<p>Intrusions are not reported in the external collector and Scrutinizer shows that no report is generated.</p> <p>Occurs when Client DPI-SSL and IPS are enabled, and the "Send Flows and Real-Time Data To External Collector" option is selected and the "External Flow Reporting Format" is set to "IPFIX with extensions", under the External Collector Settings tab on the AppFlow > Flow Reporting page.</p>	147242

Networking

Known issue	Issue ID
<p>BGP routes are still shown in the Network Routing table after the BGP neighbor is down.</p> <p>Occurs when BGP routes are established and listed in the Network > Routing page, but after SonicOS shows that the BGP router is no longer available, the page still displays the BGP routes until the firewall is restarted.</p>	163482
<p>OSPF routes are still shown in the Network Routing table after the OSPF router is down.</p> <p>Occurs when OSPF routes are established and listed in the Network > Routing page, but after SonicOS shows that the OSPF router is no longer available, the page still displays the OSPF routes until the firewall is restarted.</p>	163422
<p>A final backup interface and non-default WAN group interfaces are left without an IP address and appear to be unassigned after rebooting the firewall.</p> <p>Occurs when multiple WAN interfaces are configured using DHCP mode. All receive IP addresses initially, but those that are configured either as the final backup interface or are part of a WAN load balancing group, but not designated as the Selected interface, do not receive renewed DHCP IP addresses after the firewall restarts.</p>	160157
<p>All mirrored packets received on a WAN zone interface in Tap mode are dropped with a message including, "bounce same link pkt", preventing deep packet inspection (DPI) on the traffic to that interface. Attack traffic is not detected and logged.</p> <p>Occurs when an interface is configured in the WAN zone using Tap mode, Intrusion Prevention is enabled to detect Low Priority Attacks and then pings and low priority attack traffic are sent to the interface.</p>	158245
<p>Bandwidth management on link aggregated interfaces does not provide the total aggregated bandwidth.</p> <p>Occurs when multiple interfaces are configured for link aggregation (as a LAG), and then bandwidth management values are configured on the Advanced tab of the Edit Interface dialog. The maximum bandwidth limitation is equal to the bandwidth of a single interface, 1 Gbps.</p>	157278
<p>Cannot ping a client device on the WAN from a client connected to the LAN, and the firewall must be restarted to recover.</p> <p>Occurs when the LAN (X0) interface has no link when it is configured in Wire Mode and paired with the WAN (X1) interface, and then the link is restored.</p>	153411
<p>Link state propagation does not work with Wire Mode over link aggregation (LAG).</p> <p>Occurs when High Availability is enabled, a LAN interface is set to Wire Mode (Inspect Mode) and paired with a second LAN interface for link propagation. A third interface is aggregated with the first interface, and then a fourth interface is aggregated with the second interface. When the first interface loses connectivity to the external switch, the link status is not propagated to the second interface which unexpectedly remains up.</p>	152455

Security Services

Known issue	Issue ID
Anti-Spyware is still active after it is disabled on a zone, and spyware continues to be blocked. Occurs when Anti-Spyware has been enabled globally on the Security Services > Anti-Spyware page and then is disabled for a zone by clearing the Enable Anti-Spyware Service checkbox when editing a zone from the Network > Zones page.	140543

SSL VPN

Known issue	Issue ID
A Java error message is displayed, "Sorry, Could not connect: java.security.AccessControlException: access denied...". Occurs when accessing an SSHv1 bookmark and logging into the SSL VPN portal using Firefox from a Linux computer with Java version JRE1.8.0_25.	153694

System

Known issue	Issue ID
The firewall does not block the connection and log the event. It only logs the event. Occurs when the "Block the connection and log the event" option is selected on the Firewall Settings > SSL Control page, and the "Stateful Firewall Security" button is clicked on the System > Settings page, and the firewall is rebooted.	149003
On the Firewall Settings > Advanced Page, in the Connections panel, "DPI Connections" is selected instead of "Maximum DPI Connections" as expected. Occurs when the "DPI and Stateful Firewall Security" button is clicked on the System > Settings page, in the "One-Touch Configuration Overrides" panel, and the firewall is rebooted.	148998
On the Firewall > Access Rules page, under the Advanced tab of the Edit Rule dialog, the "Enable connection limit for each Source IP Address" option is not set as expected. It should be selected and set to 128 as specified in item 18 of the "DPI and Stateful Firewall Security" settings list on System > Settings. Occurs when the "DPI and Stateful Firewall Security" button is clicked on the System > Settings page, in the "One-Touch Configuration Overrides" panel, and the firewall is rebooted.	148994
A Java Script error is displayed. Occurs when renewing or activating a license with the manual upgrade key, then clicking the Submit button on the System > Licenses page.	147297

VPN

Known issue	Issue ID
A VPN policy cannot be created and SonicOS reports the error, "Peer ID value is not valid for Peer ID Type". Occurs when the Authentication Method is configured as "IKE using 3 rd Party Certificates" and the Local IKE ID Type and Peer IKE ID Type are set to "Distinguished name (DN)".	164561

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 supported for use with Dell SonicWALL NSA appliances running 6.1.1.12. The recommended WXA firmware version is WXA 1.3.2.


Browser support

SonicOS 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

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

 **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/>.

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 6.1 Upgrade Guide* available on MySonicWALL at <https://mysonicwall.com/> or on the Support portal at <https://support.software.dell.com/>.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to <http://software.dell.com/support/>.

The site enables you to:

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

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

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit <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 © 2015 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: 11/18/2015

232-003090-00 Rev A